DoD 5200.2-R

Personnel Security Program Regulation
Includes Change 3

23 February 1996

Foreword

This *"Personnel Security Program Regulation"* is reissued under the authority of DoD Directive 5200.2, *"DoD Personnel Security Program,"* December 20, 1979. It contains expanded direction and procedures for implementing those references cited in Chapter 1 and in Appendix A of this Regulation that pertain to acceptance and retention of DoD military, civilian, consultant and contractor personnel and of granting such persons access to classified information or assignment to a sensitive position. It also implements such recommendations from the Defense Security Review Commission Report as pertains to personnel security and approved by the Secretary of Defense.

DoD 5200.2-R, *"Department of Defense Personnel Security Program,"* December 1979, is hereby canceled as of December 31, 1986. The effective date of this Regulation is January 1, 1987.

The provisions of this Regulation apply to the Office of the Secretary of Defense (OSD) and activities supported administratively by OSD, the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and specified Commands, and the Defense Agencies.

This Regulation is mandatory for use by all DoD Components. Heads of DoD Components may issue supplementary instructions when necessary to provide for internal administration of this Regulation within their respective components.

Forward communications, including recommended changes, regarding this Regulation and copies of supplemental instructions issued, through appropriate channels to: Deputy Under Secretary of Defense for Policy, Attention: Director Counter-intelligence and Investigative Programs, Room 3C-267, The Pentagon, Washington, D.C. 203301-2200.

This Regulation is being published in Title 32, Code of Federal Regulations (CFR). DoD Components may obtain copies of this Regulation through their own publications channels. Federal Agencies and the public may obtain copies from the US. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

\Signed\
Craig Alderman, Jr.
Deputy

Chapter I

General Provisions

Section 1 -- References

1-100 -- References

(a) DoD 5200.2-R, *"DoD Personnel Security Regulation,"* December 20, 1979 (Superseded), authorized by DoD Directive 5200.2, December 20, 1979

(b) DoD 5220.22-R, *"Industrial Security Regulation,"* December 1985, authorized by DoD Directive 5220.22, December 8, 1980

(c) DoD Directive 5220.6, *"Defense Industrial Personnel Security Clearance Review Program"*, August 12, 1985

(d) Through (oo), See Appendix A

Section 2 -- Purpose and Applicability

1-200 -- Purpose

a. To establish policies and procedures to ensure that acceptance and retention of personnel in the Armed Forces, acceptance and retention of Civilian employees in the Department of Defense (DoD), and granting members of the Armed Forces, DoD civilian employees, DoD contractors, and other affiliated persons access to classified information are clearly consistent with the interests of national security.

b. This Regulation:

(1) Establishes DoD personnel security policies and procedures;

(2) Sets forth the standards, criteria and guidelines upon which personnel security determinations shall be based;

(3) Prescribes the kinds and scopes of personnel security investigations required;

(4) Details the evaluation and adverse action procedures by which personnel security determinations shall be made; and

(5) Assigns overall program management responsibilities.

1-201 -- Applicability

a. This Regulation implements the Department of Defense Personnel Security Program and takes precedence over all other departmental issuances affecting that program.

b. All provisions of the Regulation apply to DoD civilian personnel, members of the Armed Forces, excluding the Coast Guard in peacetime, contractor personnel and other personnel who are affiliated with the Department of Defense except that the unfavorable administrative action procedures pertaining to contractor personnel requiring access to classified information are contained in DoD 5220.22-R (reference (b) and in DoD Directive 5220.6 (reference (c).

c. The policies and procedures which govern the National Security Agency are prescribed by Public Laws 88-290 and 86-36, Executive Orders 10450 and 12333, DoD Directive 5210.45, Director of Central Intelligence Directive (DCID) 1/14 (references (e), (f), (g), (h), (i), and (1) respectively), and regulations of the National Security Agency.

d. Under combat conditions or other military exigencies an authority in paragraph A, Appendix F, may waive such provisions of this regulation as the circumstances warrant.

Section 3 -- Definitions

1-300 -- Access

The ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information.

1-301 -- Adverse Action

A removal from employment, suspension from employment of more than 14 days, reduction in grade, reduction of pay or furlough of 30 days or less.

1-302 -- Background Investigation (BI)

A personnel security investigation consisting of both record reviews and interviews with sources of information as prescribed in paragraph 3, Appendix B, this Regulation, covering the most recent 5 years of an individual's life or since the 18th birthday, whichever is shorter, provided that at least 2 years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

1-303 -- Classified Information

Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with the provisions of Executive Order 12356 (reference (j)).

1-304 -- Defense Central Security Index (DCSI)

An automated sub-system of the Defense Central Index of Investigations (DCII) designed to record the issuance, denial or revocation of security clearances, access to classified information, or assignment to a sensitive position by all DoD Components for military, civilian, and contractor personnel. The DCSI will serve as the central DoD repository of security related actions in order to assist DoD security officials in making sound clearance and access determinations. The DCSI shall also serve to provide accurate and reliable statistical data for senior DoD officials, Congressional committees, the General Accounting Office and other authorized Federal requesters.

1-305 -- DoD Component

Includes the Office of the Secretary of Defense; the Military Departments; Organization of the Joint Chiefs of Staff; Directors of Defense Agencies and the Unified and Specified Commands.

1-306 -- Entrance National Agency Check (ENTNAC)

A personnel security investigation scoped and conducted in the same manner as a National Agency Check except that a technical fingerprint search of the files of the Federal Bureau of Investigation is not conducted.

1-307 -- Head of DoD Component

The Secretary of Defense; the Secretaries of the Military Departments; the Chairman, Joint Chiefs of Staff; and the Commanders of Unified and Specified Commands and the Directors of Defense Agencies.

1-308 -- Immigrant Alien

Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

1-309 -- Interim Security Clearance

A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

1-310 -- Limited Access Authorization

Authorization for access to Confidential or Secret information granted to non-United States citizens and immigrant aliens, which is limited to only that information necessary to the successful accomplishment of their assigned duties and based on a background investigation scoped for 10 years (Paragraph 3, Appendix B).

1-311 -- Minor Derogatory Information

Information that, by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

1-312 -- National Agency Check (NAC)

A personnel security investigation consisting of a records review of certain national agencies as prescribed in paragraph 1, Appendix B, this Regulation, including a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI).

1-313 -- National Agency Check Plus Written Inquires (NACI)

A personnel security investigation conducted by the office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references and schools.

1-314 -- DoD National Agency Check Plus Written Inquires (DNACI)

A personnel security investigation conducted by the Defense Investigative Service (DIS) for access to ***Secret*** information consisting of a NAC, credit bureau check, and written inquires to current and former employers (see paragraph 2, Appendix B), covering a 5-year scope.

1-315 -- National Security

National security means the national defense and foreign relations of the United States.

1-316 -- Need-To-Know

A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

1-317 -- Periodic Reinvestigation (PR)

An investigation conducted every five years for the purpose of updating a previously completed background or special background investigation on persons occupying positions referred to in paragraphs 3-700 through 3-710. The scope will consist of a personal interview, NAC, LACs, credit bureau checks, employment records, employment references and developed chapter references and will normally not exceed the most recent five year period.

1-318 -- Personnel Security Investigation (PSI)

An investigation required for the purpose of determining the eligibility of DoD military and civilian personnel, contractor employees, consultants, and other persons affiliated with the Department of Defense, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSIs include investigations of affiliations with subversive organizations, suitability information, or hostage situations (see paragraph 2-403) conducted for the purpose of making personnel security determinations. They also include investigations of allegations that

arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position.

1-319 -- Scope

The time period to be covered and the sources of information to be contacted during the prescribed course of a PSI.

1-320 -- Security Clearance

A determination that a person is eligible under the standards of this Regulation for access to classified information.

1-321 -- Senior Officer of the Intelligence Community (SOIC)

The DoD Senior Officers of the Intelligence Community include: the Director, National Security Agency/Central Security Service; Director, Defense Intelligence Agency; Assistant Chief of Staff for Intelligence, U.S. Army; Assistant Chief of Staff for Intelligence, U.S Air Force; and the Director of Naval Intelligence, U.S. Navy.

1-322 -- Sensitive Position

Any position so designated within the Department of Defense, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All civilian positions are either critical-sensitive, noncritical-sensitive, or nonsensitive as described in paragraph 3-101.

1-323 -- Significant Derogatory Information

Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

1-324 -- Special Access Program

Any program imposing "need-to-know or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of persons determined to have a need-to-know.

1-325 -- Special Background Investigation (SBI)

A personnel security investigation consisting of all the components of a BI plus certain additional investigative requirements as prescribed in paragraph 4, Appendix B, this Regulation. The period of investigation for an SBI is the last 15 years or since the 18th birthday, whichever is shorter, provided that the last 2 full years are covered and that no investigation will be conducted prior to an individual's 16th birthday.

1-326 -- Special Investigative Inquiry (SII)

A supplemental personnel security investigation of limited scope conducted to prove or disprove relevant allegations that have arisen concerning a person upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a personnel security determination under the provisions of this Regulation.

1-327 -- Service

Honorable active duty (including attendance at the military academies), membership in ROTC Scholarship Program, Army and Air Force National Guard, Military Reserve Force (including active status and ready reserve), civilian employment in Government service, or civilian employment with a DoD contractor or as a consultant involving access under the DoD Industrial Security Program. Continuity of service is maintained with change from one status to another as long as there is no single break in service greater than 12 months.

1-328 -- Unfavorable Administrative Action

Adverse action taken as the result of personnel security determinations and unfavorable personnel security determinations a defined in this Regulation.

1-329 -- Unfavorable Personnel Security Determination

A denial or revocation of clearance for access to classified information; denial or revocation of access to classified information; denial or revocation of a Special Access authorization (including access to SCI); nonappointment to or nonselection for appointment to a sensitive position; nonappointment to or nonselection for any other position requiring a trustworthiness determination under this Regulation; reassignment to a position of lesser sensitivity or to a nonsensitive position; and nonacceptance for or discharge for the Armed Forces when any of the foregoing actions are based on derogatory information of personnel security significance.

1-330 -- United States Citizen (Native Born)

A person born in one of the 50 United States, Puerto Rico, Guam, American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the United States).

Chapter II

Policies

Section 1 -- Standards for Access to Classified Information or Assignment to Sensitive Duties

2-100 General

Only United States citizens shall be granted a personnel security clearance, assigned to sensitive duties, or granted access to classified information unless an authority designated in Appendix F has determined that, based on all available information, there are compelling reasons in furtherance of the Department of Defense mission, including, special expertise, to assign an individual who is not a citizen to sensitive duties or grant a Limited Access authorization to classified information. Non-U.S. citizens may be employed in the competitive service in sensitive civilian positions only when specifically approved by the Office of Personnel Management, pursuant to E.O.11935 (reference (k)). Exceptions to these requirements shall be permitted only for compelling national security reasons.

2-101 Clearance and Sensitive Position Standard

The personnel security standard that must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties is whether, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

2-102 Military Service Standard

The personnel security standard that must be applied in determining whether a person is suitable under national security criteria for appointment, enlistment, induction, or retention in the Armed Forces is that, based on all available information, there is no reasonable basis for doubting the person's loyalty to the Government of the United States.

Section 2 -- Criteria for Application of Security Standards

2-200 -- Criteria for Application of Security Standards

The ultimate decision in applying either of the security standards set forth in paragraph 2-101 and 2-102 above must be an overall common sense determination based upon all available facts. The criteria for determining eligibility for a clearance under the security standard shall include, but not be limited to the following:

a. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts threat or preparation therefore, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

b. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

c. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of Government of the United States by unconstitutional means.

d. Knowing membership with the specific intent of furthering the aims or, or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the U.S. or of any State or which seeks to overthrow the Government of the U.S. or any State or subdivision thereof by unlawful means.

e. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by Statute, Executive Order or Regulation.

f. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve or which could be expected to serve the interests of another government in preference to the interests of the U.S.

g. Disregard of public law, Statutes, Executive Orders or Regulations including violation of security regulations or practices.

h. Criminal or dishonest conduct.

i. Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

j. Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

k. Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be

(1) the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the U.S., or

(2) any other circumstances that could cause the applicant to be vulnerable.

l. Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

m. Habitual or episodic use of intoxicants to excess.

n. Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

o. Any knowing and willful falsification, coverup, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal agency.

p. Failing or refusing to answer or to authorize others to answer questions or provide information required by a congressional committee, court, or agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment.

q. Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.

Section 3 -- Types and Scope of Personnel Security Investigations

2-300 -- General

The types of personnel security investigations authorized below vary in scope of investigative effort required to meet the purpose of the particular investigation. No other types are authorized. The scope of a PSI may be neither raised nor lowered without the approval of the Deputy Under Secretary of Defense for Policy.

2-301 -- National Agency Check

Essentially, a NAC is a records check of designated agencies of the Federal Government that maintain record systems containing information relevant to making a personnel security determination. An ENTNAC is a NAC (scope as outlined in paragraph 1, Appendix b) conducted on inductees and first-term enlistees, but lacking a technical fingerprint search. A NAC is also an integral part of each BI, SBI, and Periodic Reinvestigation (PR). Chapter III prescribes when a NAC is required.

2-302 -- National Agency Check Plus Written Inquiries

The Office of Personnel Management (OPM) conducts a NAC plus Written Inquiries (NACIs) on civilian employees for all departments and agencies of the Federal Government, pursuant to E.O. 10450 reference (g)). NACIs are considered to meet the investigative requirements of this Regulation for a nonsensitive or noncritical sensitive position and/or up to a SECRET clearance and, in addition to the NAC, include coverage of law enforcement agencies, former employers and supervisors, references, and schools covering the last 5 years.

2-303 -- DoD National Agency Check Plus Written Inquiries

DIS will conduct a DNACI, consisting of the scope contained in paragraph 2, Appendix B, for DoD military and contractor personnel for access to SECRET information. Chapter III prescribes when a DNACI is required.

2-304 -- Background Investigation

The BI is the principal type of investigation conducted when an individual requires TOP Secret clearance or is to be assigned to a critical sensitive position. The BI normally covers a 5-year period and consists of a subject interview, NAC, LACs, credit checks, developed character references (3), employment records checks, employment references (3), and select scoping as required to resolve unfavorable or questionable information. (See paragraph 3, Appendix B). Chapter III prescribes when a BI is required.

2-305 -- Special Background Investigation

a. An SBI is essentially a BI providing additional coverage both in period of time as well as sources of information, scoped in accordance with the provisions of DCID 1/14 (reference (1)) but without the personal interview. While the kind of coverage provided for by the SBI determines eligibility for access to SCI, DoD has adopted this coverage for certain other Special Access programs. Chapter III prescribes when an SBI is required.

b. The OPM, FBI, Central Intelligence Agency (CIA), Secret Service, and the Department of State conduct specially scoped BIs under the provisions of DCID 1/14. Any investigation conducted by one of the above-cited agencies under DCID 1/14 standards is considered to meet the SBI investigative requirements of this Regulation.

c. The detailed scope of an SBI is set forth in paragraph 4, Appendix B.

2-306 -- Special Investigative Inquiry

a. A Special Investigative Inquiry is a personnel security investigation conducted to prove or disprove allegations relating to the criteria outlined in paragraph 2-200 of this Regulation, except current criminal activities (see paragraph 2-402d), that have arisen concerning an individual upon whom a personnel security determination has been previously made and who, at the time of the allegation, holds a security clearance or otherwise occupies a position that requires a trustworthiness determination.

b. Special Investigative Inquiries are scoped a necessary to address the specific matters requiring resolution in the case concerned and generally consist of record checks and/or interviews with potentially knowledgeable persons. An SII may include an interview with the subject of the investigation when necessary to resolve conflicting information and/or to provide an opportunity to refute or mitigate adverse information.

c. In those cases when there is a disagreement between Defense Investigative Service (DIS) and the requester as to the appropriate scope of the investigation, the matter may be referred to the Deputy Under Secretary of Defense for Policy for resolution.

2-307 -- Periodic Reinvestigation

As referred to in paragraph 3-700 and other national directives, certain categories of duties, clearance, and access require the conduct of a PR every five years according to the scope outlined in paragraph 5, Appendix B. The PR scope applies to military, civilian, contractor, and foreign national personnel.

2-308 -- Personal Interview

Investigative experience over the years has demonstrated that, given normal circumstances, the subject of a personnel security investigation is the best source of accurate and relevant information concerning the matters under consideration. Further, restrictions imposed by the Privacy Act of 1974 (reference (m)) dictate that Federal investigative agencies collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs. Accordingly, personal interviews are an integral part of the DoD personnel security program and shall be conducted in accordance with the requirements set forth in the following paragraphs of this section.

a. ***BI/PR***

A personal interview shall be conducted by a trained DIS agent as part of each BI and PR.

b. ***Resolving Adverse Information***

A personal interview of the subject shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in this Regulation to conduct personnel security investigations), when necessary, as part of each Special Investigative Inquiry, as well as during the course of initial or expanded investigations, to resolve or clarify any information which may impugn the subject's moral character, threaten the subject's future federal employment, raise the question of subject's security clearability, or be otherwise stigmatizing.

c. ***Hostage Situation***

A personal interview shall be conducted by a DIS agent (or, when authorized, by investigative personnel of other DoD investigative organizations designated in the Regulation to conduct personnel security investigations) in those instances in which an individual has immediate family members or other persons bound by ties of affection or obligation who reside in a nation whose interests are inimical to the interests of the United States. (See paragraph 2-403.)

d. ***Applicants/Potential Nominees for DoD Military or Civilian Positions Requiring Access to SCI or Other Positions Requiring an SBI***

A personal interview of the individual concerned shall be conducted, to the extent feasible, as part of the selection process for applicants/potential nominees for positions requiring access to SCI or completion of an SBI. The interview shall be conducted by a designee of the Component to which the applicant or potential nominee is assigned. Clerical personnel are

not authorized to conduct these interviews. Such interviews shall be conducted utilizing resources in the order of priority indicated below:

(1) Existing personnel security screening systems (e.g., Air Force Assessment Screening Program, Naval Security Group Personnel Security Interview Program, U.S. Army Personnel Security Screening Program); or

(2) Commander of the nominating organization or such official as he or she has designated in writing (e.g., Deputy Commander, Executive Officer, Security Officer, Security Manager, S-2, Counter-intelligence Specialist, Personnel Security Specialist, or Personnel Officer); or

(3) Agents of investigative agencies in direct support of the Component concerned.

e. ***Administrative Procedures***

(1) The personal interview required by paragraph d., above, shall be conducted in accordance with Appendix G.

(2) For those investigations requested subsequent to the personal interview requirements of paragraph d., above, the following procedures apply:

(a) The DD Form 1879 (**Request for Personnel Security Investigation**) shall be annotated under Item 20 (Remarks) with the statement "Personal Interview Conducted by (cite the duty assignment of the designated official (e.g., Commander, Security Officer, Personnel Security Specialist, etc.))" in all cases in which an SBI is subsequently requested.

(b) Unfavorable information developed through the personal interview required by paragraph d., above, will be detailed in a written report attached to the DD Form 1879 to include full identification of the interviewer. Failure to provide such information may result in conduct of an incomplete investigation by DIS.

(c) Whenever it is determined that it is not feasible to conduct the personal interview required by paragraph d. above, prior to requesting the SBI, the DD Form 1879 shall be annotated under Item 20 citing the reason for not conducting the interview.

2-309 -- Expanded Investigation

If adverse or questionable information relevant to a security determination is developed during the conduct of a personnel security investigation, regardless of type, the investigation shall be expanded, consistent with the restrictions in paragraph 2-504, to the extent necessary to substantiate or disprove the adverse or questionable information.

Section 4 -- Authorized Personnel Security Investigative Agencies

2-400 -- General

The DIS provides a single centrally directed personnel security investigative service to conduct personnel security investigations within the 50 states, District of Columbia, and Commonwealth of Puerto Rico for DoD Components, except as provided for in DoD Directive 5100.23 (reference (n)). DIS will request the Military Departments or other appropriate Federal Agencies to accomplish DoD investigative requirements in other geographic areas beyond their jurisdiction. No other DoD Component shall conduct personnel security investigations unless specifically authorized by the Deputy Assistant Secretary of Defense (Intelligence and Security). In certain instances provided for below, the DIS shall refer an investigation to other investigative agencies.

2-401 -- Subversive Affiliations

a. ***General***. In the context of DoD investigative policy, subversion refers only to such conduct as is forbidden by the laws of the United States. Specifically, this is limited to information concerning the activities of individuals or groups that involve or will involve the violation of Federal law, for the purpose of:

(1) Overthrowing the Government of the United States or the government of a state;

(2) Substantially impairing for the purpose of influencing U.S. Government policies or decisions:

(a) The functions of the Government of the United States, or
(b) The functions of the government of a state;

(3) Depriving persons of their civil rights under the Constitution or laws of the United States.

b. ***Military Department/FBI Jurisdiction***. Allegations of activities covered by criteria a. through f. of paragraph 2-200 of this Regulation are in the exclusive investigative domain of either the counterintelligence agencies of the Military Departments or the FBI, depending on the circumstances of the case and the provisions of the Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the FBI (reference (o)). Whenever allegations of this nature are developed, whether before or after a security clearance has been issued or during the course of a personnel security investigation conducted by DIS, they shall be referred immediately to either the FBI or to a military department counterintelligence agency as appropriate.

c. ***DIS Jurisdiction***. Allegations of activities limited to those set forth in criterion g. through q. of paragraph 2-200 of this Regulation shall be investigated by DIS.

2-402 -- Suitability Information

a. ***General***. Most derogatory information developed through personnel security investigations of DoD military or civilian personnel is so-called suitability information, that is, information pertaining to activities or situations covered by criteria g. through q. of paragraph 2-200 of this Regulation. Almost all unfavorable personnel security determinations made by DoD authorities are based on derogatory suitability information, although such information is often used as a

basis for unfavorable administrative actions not of a security nature, such as action under the Uniform Code of Military Justice or removal from Federal employment under OPM regulations.

b. ***Pre-clearance Investigation***. Derogatory suitability information, except that covered in d. below, developed during the course of a personnel security investigation, prior to the issuance of an individual's personnel security clearance, shall be investigated by DIS to the extent necessary to confirm or refute its applicability to criteria g. through q. of paragraph 2-200.

c. ***Postadjudicative Investigation***. Derogatory suitability allegations, except those covered by d. below, arising subsequent to clearance requiring investigation to resolve and to determine the individual's eligibility for continued access to classified information, reinstatement of clearance/access, or retention in a sensitive position shall be referred to DIS to conduct a Special Investigative Inquiry. Reinvestigation of individuals for adjudicative reconsideration due to the passage of time or evidence of favorable behavior shall also be referred to DIS for investigation. In such cases, completion of the appropriate statement of personal history by the individual constitutes consent to be investigated. Individual consent or completion of a statement of personal history is not required when paragraph 3-701 applies. Postadjudiction investigation of allegations of a suitability nature required to support other types of unfavorable personnel security determinations or disciplinary procedures independent of a personnel security determination shall be handled in accordance with applicable Component administrative regulations. These latter categories of allegations lie outside the DoD personnel security program and are not a proper investigative function for departmental counterintelligence organizations, Component personnel security authorities, or DIS.

d. ***Allegations of Criminal Activity***. Allegations of possible criminal conduct arising during a personnel security investigation shall be referred to the appropriate Department of Defense criminal investigative agency, Military Department or civilian jurisdiction unless the limitations in paragraph 2-402d(1) through 2-402d(3) below, apply. Where the allegation concerns a potential violation of the Uniform Code of Military Justice, Military Department investigative Agencies have primary investigative jurisdiction. The following limitations apply to referrals to all law enforcement agencies, both military and civilian.

(1) Allegations shall not be referred or reported to law enforcement agencies where agreements with the agency or in cases where there is no agreement, past experience indicates that the jurisdiction does not have a substantial interest in prosecution of the offense or in receiving reports of the offense either due to the type or offense involved or the circumstances under which it occurred.

(2) Allegations about private consensual sexual acts with adults shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. That limitation does not apply to allegations that an individual attempted, solicited, or committed a criminal offense in the following circumstances:

(a) By using force, coercion, or intimidation.

(b) With a person under 17 years of age.

(c) Openly in public view.

(d) For compensation or with an offer of compensation to another individual.

(e) While on active duty in, or on duty in a Reserve component of, the Armed Forces of the United States and

1. Aboard a military vessel or aircraft; or

2. With a subordinate in circumstances that violate customary military superior-subordinate relationships.

Exceptions to that limitation will be made only with the specific written authorization of the General Counsel of the Department of Defense, or his or her designee.

(3) Information about an individual's sexual orientation or statements by an individual that he or she is a homosexual or bisexual, or words to that effect, shall not be referred or reported to law enforcement agencies or to Military Departments (other than consolidated adjudication facilities) for any purpose. If investigative reports containing such information are referred to law enforcement agencies or Military Departments for other reasons, information subject to the limitations in this paragraph will be removed.

2-403 -- Hostage Situations

a. ***General***. A hostage situation exists when a member of subject's immediate family or such other person to whom the individual is bound by obligation or affection resides in a country whose interests are inimical to the interests of the United States. The rationale underlying this category of investigation is based on the possibility that an individual in such a situation might be coerced, influenced, or pressured to act contrary to the interests of national security.

b. ***DIS Jurisdiction***. In the absence of evidence of any coercion, influence or pressure, hostage investigations are exclusively a personnel security matter, rather than counterintelligence, and all such investigations shall be conducted by DIS.

c. ***Military Department and/or FBI Jurisdiction***. Should indications be developed that hostile intelligence is taking any action specifically directed against the individual concerned -- or should there exist any other evidence that the individual is actually being coerced, influenced, or pressured by an element inimical to the interests of national security -- then the case becomes a counterintelligence matter (outside of investigative jurisdiction of DIS) to be referred to the appropriate military department or the FBI for investigation.

2-404 -- Overseas Personnel Security Investigations

Personnel security investigations requiring investigation overseas shall be conducted under the direction and control of DIS by the appropriate military department investigative organization. Only postadjudication investigations involving an overseas subject may be referred by the requester directly to the military department investigative organization having investigative responsibility in the overseas area concerned (see Appendix J) with a copy of the investigative

request sent to DIS. In such cases, the military department investigative agency will complete the investigation, forward the completed report of investigation directly to DIS, with a copy to the requester.

Section 5 -- Limitations and Restrictions

2-500 -- Authorized Requesters and Personnel Security Determination Authorities

Personnel security investigations may be requested and personnel security clearances (including Special Access authorizations as indicated) granted only by those authorities designated in paragraph 5-101 and Appendix F.

2-501 -- Limit Investigations and Access

The number of persons cleared for access to classified information shall be kept to a minimum, consistent with the requirements of operations. Special attention shall be given to eliminating unnecessary clearances and requests for personnel security investigations.

2-502 -- Collection of Investigative Data

To the greatest extent practicable, personal information relevant to personnel security determinations shall be obtained directly from the subject of a personnel security investigation. Such additional information required to make the necessary personnel security determination shall be obtained as appropriate from knowledgeable personal sources, particularly subject's peers, and through checks of relevant records including school, employment, credit, medical, and law enforcement records.

2-503 -- Privacy Act Notification

Whenever personal information is solicited from an individual preparatory to the initiation of a personnel security investigation, the individual must be informed of

(1) the authority (statute or Executive order that authorized solicitation);

(2) the principal purpose or purposes for which the information is to be used;

(3) the routine uses to be made of the information;

(4) whether furnishing such information is mandatory or voluntary;

(5) the effect on the individual, if any, of not providing the information and

(6) that subsequent use of the data may be employed as part of an aperiodic, random process to screen and evaluate continued eligibility for access to classified information.

2-504 -- Restrictions on Investigators

Investigations shall be carried out insofar as possible to collect only as much information as is relevant and necessary for a proper personnel security determination. Questions concerning personal and domestic affairs, national origin, financial matters, and the status of physical health should be avoided unless the question is relevant to the criteria of paragraph 2-200 of this Regulation. Similarly, the probing of a person's thoughts or beliefs and questions about conduct that have no personnel security implications are unwarranted. When conducting investigations under the provisions of this Regulation, investigators shall:

a. Investigate only cases or persons assigned within their official duties.

b. Interview sources only where the interview can take place in reasonably private surroundings.

c. Always present credentials and inform sources of the reasons for the investigation. Inform sources of the subject's accessibility to the information to be provided and to the identity of the sources providing the information. Restrictions on investigators relating to Privacy Act advisements to subjects of personnel security investigations are outlined in paragraph 2-503.

d. Furnish only necessary identity data to a source, and refrain from asking questions in such a manner as to indicate that the investigator is in possession of derogatory information concerning the subject of the investigation.

e. Refrain from using, under any circumstances, covert or surreptitious investigative methods, devices, or techniques including mail covers, physical or photographic surveillance, voice analyzers, inspection of trash, paid informants, wiretap, or eavesdropping devices.

f. Refrain from accepting any case in which the investigator knows of circumstances that might adversely affect his fairness, impartiality, or objectivity.

g. Refrain, under any circumstances, from conducting physical searches of subject or his property.

h. Refrain from attempting to evaluate material contained in medical files. Medical files shall be evaluated for personnel security program purposes only by such personnel as are designated by DoD medical authorities. However, review and collection of medical record information may be accomplished by authorized investigative personnel.

2-505 -- Polygraph Restrictions

The polygraph may be used as a personnel security screening measure only in those limited instances authorized by the Secretary of Defense in DoD Directive 5210.48, (reference (p)).

(b) ***NACI:*** Civilian employees
(c) ***ENTNAC:*** First-term enlistees

(2) ***Interim Clearance:***

(a) When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in subparagraphs (b) through (e) below, have been complied with.

(b) Favorable review of DD Form 398-2/SF-85/SF-171/DD Form 48.

(c) NACI, DNACI, or ENTNAC initiated.

(d) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(e) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.

c. ***Confidential***

(1) ***Final Clearance***:

(a) ***NAC or ENTNAC:*** Military and contractor employees (except for Philippine national members of the United States Navy on whom a BI shall be favorably completed.)

(b) ***NACI:*** Civilian employees (except for summer hires who may be granted a final clearance on the basis of a NAC).

(2) ***Interim Clearance***

(a) Favorable review of DD Form 398-2/SF 85/SF 171/DD Form 48.

(b) NAC, ENTNAC or NACI initiated.

(c) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(d) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.

d. ***Validity of Previously Granted Clearances:***

Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is required, investigative requirements of this directive will be followed.

Chapter III

Personnel Security Investigative Requirements

Section 1 -- Sensitive Positions

3-100 -- Designation of Sensitive Positions

Certain civilian positions within the Department of Defense entail duties of such a sensitive nature, including access to classified information, that the misconduct, malfeasance, or nonfeasance of an incumbent in any such position could result in an unacceptable adverse impact upon the national security. These positions are referred to in this Regulation as sensitive positions. It is vital to the national security that great care be exercised in the selection of individuals to fill such positions. Similarly, it is important that only positions which truly meet one or more of the criteria set forth in paragraph 3-101 be designated as sensitive.

3-101 -- Criteria for Security Designation of Positions

Each civilian position within the Department of Defense shall be categorized, with respect to security sensitivity, as either nonsensitive, noncritical-sensitive, or critical-sensitive.

a. The criteria to be applied in designating a position as sensitive are:

(1) ***Critical-sensitive***

(a) Access to Top Secret information.

(b) Development or approval of plans, policies, or programs that effect the overall operations of the Department of Defense or of a DoD Component.

(c) Development or approval of war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war.

(d) Investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations.

(e) Fiduciary, public contact, or other duties demanding the highest degree of public trust.

(f) Duties falling under Special Access programs.

(g) Category I automated data processing (ADP) positions.

(h) Any other position so designated by the head of the Component or designee.

(2) ***Noncritical-sensitive***

(a) Access to Secret or Confidential information.

(b) Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DoD personnel and property.

(c) Category II automated data processing positions.

(d) Duties involving education and orientation of DoD personnel.

(e) Duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DoD personnel and property.

(f) Any other position so designated by the head of the Component or designee.

b. All other positions shall be designated as nonsensitive.

3-102 -- Authority to Designate Sensitive Positions

The authority to designate sensitive positions is limited to those authorities designated in paragraph G, Appendix F. These authorities shall designate each position within their jurisdiction as to its security sensitivity and maintain these designations current vis-à-vis the specific duties of each position.

3-103 -- Limitation of Sensitive Positions

It is the responsibility of those authorities authorized to designate sensitive positions to insure that (1) only those positions are designated as sensitive that meet the criteria of paragraph 3-101 above and (2) that the designation of sensitive positions is held to a minimum consistent with mission requirements. Designating authorities shall maintain an accounting of the number of sensitive positions by category, i.e., critical or non-critical sensitive. Such information will be included in annual report required in Chapter XI.

3-104 -- Billet Control System for Top Secret

a. To standardize and control the issuance of Top Secret clearances within the Department of Defense, a specific designated billet must be established and maintained for all DoD military and civilian positions requiring access to Top Secret information. Only persons occupying these billet positions will be authorized a Top Secret clearance. If an individual departs from a Top Secret billet to a billet/position involving a lower level clearance, the Top Secret clearance will be administratively rescinded. This Top Secret billet requirement is in addition to the existing billet structure maintained for SCI access.

b. Each request to DIS for a BI or SBI that involves access to Top Secret or SCI information will require inclusion of the appropriate billet reference, on the request for investigation. Each Component head should incorporate, to the extent feasible, the Top Secret billet structure into the component Manpower Unit Manning Document. Such a procedure should minimize the time and effort required to maintain such a billet structure.

c. A report on the number of established Top Secret billets will be submitted each year to the DUSD(P) as part of the annual clearance report referred to in Chapter XI.

Section 2 -- Civilian Employment

3-200 -- General

The appointment of each civilian employee in any DoD Component is subject to investigation, except for reappointment when the break in employment is less than 12 months. The type of investigation required is set forth in this section according to position sensitivity.

3-201 -- Nonsensitive Positions

In accordance with the OPM Federal Personnel Manual, (reference (cc)) a NACI shall be requested not later than 3 working days after a person is appointed to a nonsensitive position. Although there is normally no investigation requirement for per diem, intermittent, temporary or seasonal employees in nonsensitive positions provided such employment does not exceed an aggregate of 120 days in either a single continuous or series of appointments, a NAC may be requested of DIS where deemed appropriate by the employing activity.

3-202 -- Noncritical-sensitive Positions

a. An NACI shall be requested and the NAC portion favorably completed before a person is appointed to a noncritical-sensitive position (for exceptions see paragraph 3-204). An ENTNAC, NAC or DNACI conducted during military or contractor employment may also be used for appointment provided a NACI has been requested from OPM and there is no more than 12 months break in service since completion of the investigation.

b. Seasonal employees (including summer hires) normally do not require access to classified information. For those requiring access to classified information the appropriate investigation is required. The request for the NAC (or NACI) should be submitted to DIS by entering "SH" (summer hire) in red letters approximately one inch high on the DD Form 398-2, Personnel Security Questionnaire (National Agency Checklist). Additionally, to ensure expedited processing by DIS, summer hire requests should be assembled and forwarded to DIS in bundles, when appropriate.

3-203 -- Critical-Sensitive Positions

A BI shall be favorably completed prior to appointment to critical-sensitive positions (for exceptions see paragraph 3-204). Certain critical-sensitive positions require a preappointment SBI in accordance with Section 5 of this chapter. Preappointment BIs and SBIs will be conducted by DIS.

3-204 -- Exceptions

a. ***Noncritical-Sensitive***

In an emergency, a noncritical-sensitive position may be occupied pending the completion of the NACI if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made part of the record. In such instances, the position may be filled only after the NACI has been requested.

b. ***Critical-sensitive***

In an emergency, a critical-sensitive position may be occupied pending completion of the BI (or SBI, as appropriate) if the head of the requesting organization finds that the delay in appointment would be harmful to the national security and such finding is reduced to writing and made a part of the record. In such instances, the position may be filled only when the NAC portion of the BI (or SBI) or a previous valid NACI, NAC or ENTNAC has been completed and favorably adjudicated.

3-205 -- Mobilization of DoD Civilian Retirees

The requirements contained in paragraph 3-200 of this section, regarding the type of investigation required by position sensitivity for DoD civilian retirees temporary appointment when the break in employment is greater than 12 months, should either be expedited or waived for the purposes of mobilizing selected reemployed annuitants under the provisions of Title 5, United States Code, depending upon the degree of sensitivity of the position to which assigned. Particular priority should be afforded to newly assigned personnel assigned to the defense intelligence and security agencies with respect to granting security clearances in an expeditious manner under paragraph 3-200 of this section.

Section 3 -- Military Appointment, Enlistment, and Induction

3-300 -- General

The appointment, enlistment, and induction of each member of the Armed Forces or their Reserve Components shall be subject to the favorable completion of a personnel security investigation. The types of investigation required are set forth in this section.

3-301 -- Entrance Investigation

a. An ENTNAC shall be conducted on each enlisted member of the Armed Forces at the time of initial entry into the service. A DNACI shall be conducted on each commissioned officer, except as permitted by paragraph 3-303 of this section, warrant officer, cadet, midshipman, and Reserve Officers Training Candidate, at the time of appointment. A full NAC shall be conducted upon reentry of any of the above when there has been a break in service greater than 12 months.

b. If an officer or warrant officer candidate has been the subject of a favorable NAC or ENTNAC and there has not been a break in service of more than 12 months, a new NAC is not authorized. This includes ROTC graduates who delay entry onto active duty pending completion of their studies.

c. All derogatory information revealed during the enlistment or appointment process that results in a moral waiver will be fully explained on a written summary attached to the DD Form 398-2.

3-302 -- Reserve Components and National Guard

Reserve Component and National Guard personnel not on active duty are subject to the investigative requirements of this chapter.

3-303 -- Exceptions for Certain Commissioned Officers of Reserve Components

The requirements for entrance investigation shall be rigidly adhered to except as follows. Health professionals, chaplains, and attorneys may be commissioned in the Reserve Components prior to completion of a DNACI provided that:

a. A DNACI is initiated at the time an application for a commission is received; and

b. The applying health professional, chaplain, or attorney agrees in writing that, if the results of the investigation are unfavorable, he or she will be subject to discharge if found to be ineligible to hold a commission. Under this exception, commissions in Reserve Components other than the National Guard may be tendered to immigrant alien health professionals, chaplains, and attorneys.

3-304 -- Mobilization of Military Retirees

The requirements contained in paragraph 3-301 of this section, regarding a full NAC upon reentry to active duty of any officer or enlisted regular/reserve military retiree or Individual Ready Reserve who has been separated from service for a period of greater than 12 months, should be waived for the purposes of partial or full mobilization under provisions of Title 10 (Title 14, pertaining to the US Coast Guard as an element of the Navy) United States Code, to include the period of prescribed service refresher training. Particular priority should be afforded to military retirees mobilized and assigned to the defense intelligence and security agencies communities.

Section 4 -- Security Clearance

3-400 -- General

a. The authorities designated in paragraph A, Appendix F are the only authorities authorized to grant, deny or revoke DoD personnel security clearances. The granting of such clearances shall be limited to only those persons who require access to classified information for mission accomplishment.

b. Military, DoD civilian, and contractor personnel who are employed by or serving in a consultant capacity to the DoD, may be considered for access to classified information only when such access is required in connection with official duties. Such individuals may be granted either a final or interim personnel security clearance provided the investigative requirements set forth below are complied with, and provided further that all available information has been

adjudicated and a finding made that such clearance would be clearly consistent with the interests of national security.

3-401 -- Investigative Requirements for Clearance

a. ***Top Secret***

(1) ***Final Clearance***

(a) BI
(b) Established billet per paragraph 3-104 (except contractors)

(2) ***Interim Clearance***

(a) Favorable NAC, ENTNAC, DNACI, or NACI completed

(b) Favorable review of DD Form 398/SF-86/SF-171/DD Form 49

(c) BI or SBI has been initiated

(d) Favorable review of local personnel, base/military police, medical, and other security records as appropriate.

(e) Established billet per paragraph 3-104 (except contractors)

(f) Provisions of paragraph 3-204 have been met regarding civilian personnel.

b. ***Secret***

(1) ***Final Clearance***

(a) ***DNACI:*** Military (except first-term enlistees) and contractor employees
(b) ***NACI:*** Civilian employees
(c) ***ENTNAC:*** First-term enlistees

(2) ***Interim Clearance***

(a) When a valid need to access Secret information is established, an interim Secret clearance may be issued in every case, provided that the steps outlined in subparagraphs (b) through (e) below, have been complied with.

(b) Favorable review of DD Form 398-2/SF-85/SF-171/DD Form 48.

(c) NACI, DNACI, or ENTNAC initiated.

(d) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(e) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.

c. ***Confidential***

(1) ***Final Clearance***

(a) ***NAC or ENTNAC:*** Military and contractor employees (except for Philippine national members of the United States Navy or whom a BI shall be favorably completed.)

(b) ***NACI:*** Civilian employees (except for summer hires who may be granted a final clearance on the basis of a NAC).

(2) ***Interim Clearance***

(a) Favorable review of DD Form 398-2/SF-85/SF-171/DD Form 48.

(b) NAC, ENTNAC or NACI initiated.

(c) Favorable review of local personnel, base military police, medical, and security records as appropriate.

(d) Provisions of paragraph 3-204 have been complied with regarding civilian personnel.

d. ***Validity of Previously Granted Clearances***

Clearances granted under less stringent investigative requirements retain their validity; however, if a higher degree of clearance is required, investigative requirements of this directive will be followed.

3-402 -- Access to Classified Information by Non-U.S. Citizens

a. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to an immigrant alien or a foreign national. Such individuals may be granted a "Limited Access Authorization" (LAA) in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed in pursuit of a specific DoD requirement involving access to specified classified information for which a cleared or clearable U.S. citizen is not available.

b. ***Limitations***

(1) LAAs shall be limited only to individuals who have a special skill or technical expertise essential to the fulfillment of a DoD requirement that cannot reasonably be filled by a U.S. citizen.

(2) LAAs shall not be granted to personnel who perform routine administrative or other support duties, such as secretaries, clerks, drivers, or mechanics, unless it has been clearly established that those duties cannot be performed by a U.S. citizen.

(3) Personnel granted LAAs shall not be permitted uncontrolled access to areas where classified information is stored or discussed. Classified information shall be maintained in a location that will be under the continuous control and supervision of an appropriately cleared U.S. citizen.

(4) LAA personnel shall not be designated as a courier or escort for classified material outside the location in which access is permitted unless they are accompanied by an appropriately cleared U.S. person.

c. ***Authorized Access Levels***

(1) LAAs may be granted only at the ***Secret*** and ***Confidential*** level. LAAs for ***Top Secret*** are prohibited. Interim access is not authorized pending approval of a LAA.

(2) The information the non-U.S. citizen may have access to must be approved for release to the person's country or countries of citizenship, in accordance with DoD Directive 5230.11 (reference (ll.)).

(3) Access to classified information shall be limited or related to a specific program or project; the LAA shall be canceled or rejustified as described herein upon completion of the program or project.

(4) Access to classified information outside the scope of the approved LAA shall be considered a compromise of classified information and shall be investigated, in accordance with DoD 5200.1-R (reference (q)).

d. ***Requirements***

(1) The LAA granting authority (Appendix F) may consider issuing an LAA only after a written determination is made that access is essential for a critical mission and no U.S. citizen is available to perform the duties.

(2) When a non-U.S. citizen who is nominated for an LAA is a citizen of a country with which the United States has an agreement providing for security assurances based on that country's investigative requirements, which are commensurate with the standards provided herein, an LAA may be issued at the requisite level.

(3) In addition to the above, a favorably completed (within the last 5 years) and adjudicated SSBI is required prior to granting an LAA. If the SSBI cannot provide full investigative coverage, a polygraph examination (if there are no host country legal prohibitions) to resolve the remaining personnel security issues (See DoD Directive 5210.48 (reference (p)), must be favorably completed before granting access.

(4) If geographical, political or medical situations prevent the full completion of the SSBI or prevent the polygraph examination to supplement a less than full SSBI, a LAA may be granted only with approval of the ASD(C3I).

(5) If an LAA is withdrawn and the individual subsequently is considered for an LAA, the provisions of this paragraph shall apply concerning an SSBI and polygraph examination. The scope of the SSBI normally shall cover the period since the previous background investigation or 10 years, whichever is shorter.

(6) A PR shall be conducted on every individual with a LAA 5 years from the date of the last PR or SSBI, as appropriate.

(7) All requests for initial LAAs shall contain a detailed justification and plan describing the following:

(a) The location of the classified material (security containers) in relationship to the location of the foreign national.

(b) The compelling reason for not employing a cleared or clearable U.S. citizen.

(c) A synopsis of an annual continuing assessment program to evaluate the individual's continued trustworthiness and eligibility for access.

(d) A plan to control access to secure areas and to classified and controlled unclassified information.

e. ***LAA Determination Authority***

(1) LAA determinations may only be made by an official listed in paragraph B, Appendix F. The designated single authorizing official for the Military Departments, the Unified Combatant Commands, and the DIS precludes an LAA determination by any other official at the major command level, or equivalent.

(2) LAA determinations for employees of the Military Departments shall be the sole authority of the Secretary of the Military Department or a single designee such as the Service central adjudication facility. Field elements must submit their recommendations for access to the designated official for approval, along with affiliated information in support of the action.

(3) The Commander of a Unified Combatant Command, or single designee (flag officer or civilian equivalent) responsible for implementation of the personnel security program, shall be authorized to issue, deny, or revoke an LAA. LAA determinations by the Unified Combatant Commands shall be reported to the central adjudicative facility of the Military Department in accordance with the assigned responsibilities in DoD Directive 5100.3 (reference (mm)) for inclusion in the DCII.

(4) All LAA determinations, favorable and unfavorable, shall be entered into the DCII.

(5) The administrative action procedures in Chapter 8 do not apply to LAA determinations.

f. ***Record***

(1) The LAA granting authority shall ensure that a record is created on issuance and maintained for 5 years from the date the LAA ceases. The record shall include the following:

(a) The identity of the individual granted the LAA, to include the full name, date and place of birth, current citizenship(s), any SSN, and any national identifying number issued by the individual's country or countries of citizenship;

(b) The individual's status as an immigrant alien or foreign national; if an immigrant alien, the date and place such status was granted;

(c) The classification level of the LAA; i.e., ***Secret*** or ***Confidential***;

(d) Date and type of most recent background investigation or PR and the investigating Agency.

(e) Whether a polygraph examination was conducted; if so, the date and administering Agency for the most recent examination.

(f) The nature and identity of the classified program materials to which access is authorized and the precise duties performed.

(g) The compelling reasons for granting access to the information.

(2) All LAA SSBIs and PRs shall be conducted under the auspices of the DIS and shall comply with the requirements of Appendix B. The DIS shall initiate leads to the respective Military Department investigative agencies overseas as well as the Department of State (DOS). The results of all investigations, to include those conducted by the DOS, shall be returned to the DIS for review and entry into the DCII and return to the designated granting official for adjudication. (To expedite matters, the investigation may be initiated locally provided the necessary paperwork has been submitted to the DIS for assignment of a case control number and initiation of such other checks as needed.)

(3) The Unified Combatant Commands shall report LAAs they issue to the applicable DoD Component CAF for entry into the DCII. The Unified Combatant Commands shall ensure that all investigative paperwork for the initiation of the SSBI or PR is submitted to the DIS through the designated single-approval authority responsible for adjudication and issuance of the LAA.

(4) All LAA nominees must agree to undergo a polygraph examination at any time during the period the LAA is in effect, if there is no host-country legal prohibition.

g. All LAAs shall be reviewed annually by the issuing component to determine if continued access is in compliance with DoD policy. A report on all LAAs in effect, including the data required in paragraph 3-402.f.(l) shall be furnished to the DASD(I&S) within 60 days after the end of each fiscal year (see subsection 11-102 below).

3-403 -- Access by Persons Outside the Executive Branch

a. Access to classified information by persons outside the Executive Branch shall be accomplished in accordance with Chapter VII, DoD 5200.1-R (reference (q)). The investigative requirement shall be the same as for the appropriate level of security clearance, except as indicated below.

b. Members of the U.S. Senate and House of Representative do not require personnel security clearances. They may be granted access to DoD classified information which relates to matters under the jurisdiction of the respective Committees to which they are assigned and is needed to perform their duties in connection with such assignments.

c. Congressional staff members requiring access to DoD classified information shall be processed for a security clearance in accordance with DoD Directive 5142.1 (reference (oo)) and the provisions of this Regulation. The Director, Washington Headquarters Services (WHS) will initiate the required investigation (initial or reinvestigation) to DIS, adjudicate the results and grant, deny or revoke the security clearance, as appropriate. The Assistant Secretary of Defense (Legislative Affairs) will be notified by WHS of the completed clearance action.

d. State governors do not require personnel security clearances. They may be granted access to specifically designated classified information, on a "need-to-know" basis, based upon affirmation by the Secretary of Defense or the head of a DoD Component or single designee, that access, under the circumstances, serves the national interest. Staff personnel of a governor's office requiring access to classified information shall be investigated and cleared in accordance with the prescribed procedures of this Regulation when the head of a DoD Component, or single designee, affirms that such clearance serves the national interest. Access shall also be limited to specifically designated classified information on a "need-to-know" basis.

e. Members of the U.S. Supreme Court, the Federal judiciary and the Supreme Courts of the individual states do not require personnel security clearances. They may be granted access to DoD classified information to the extent necessary to adjudicate cases being heard before these individual courts.

f. Attorneys representing DoD military, civilian or contractor personnel, requiring access to DoD classified information to properly represent their clients, shall normally be investigated by DIS and cleared in accordance with the prescribed procedures in paragraph 3-401. This shall be done upon certification of the General Counsel of the DoD Component involved in the litigation that access to specified classified information, on the part of the attorney concerned, is necessary to adequately represent his or her client. In exceptional instances, when the exigencies of a given situation do not permit timely compliance with the provisions of paragraph 3-401, access may be granted with the written approval of an authority designated in Appendix F provided that as a minimum:

(a) a favorable name check of the FBI and the DCII has been completed, and
(b) a DoD Non-Disclosure Agreement has been executed.

In post-indictment cases, after a judge has invoked the security procedures of the Classified Information Procedures Act (CIPA) (reference (m)), the Department of Justice may elect to

conduct the necessary background investigation and issue the required security clearance, in coordination with the affected DoD Component.

3-404 -- Restrictions on Issuance of Personnel Security Clearances

Personnel security clearances must be kept to the absolute minimum necessary to meet mission requirements.

Personnel security clearances shall normally not be issued:

a. To persons in nonsensitive positions.

b. To persons whose regular duties do not require authorized access to classified information.

c. For ease of movement of persons within a restricted, controlled, or industrial area, whose duties do not require access to classified information.

d. To persons who may only have inadvertent access to sensitive information or areas, such as guards, emergency service personnel, firemen, doctors, nurses, police, ambulance drivers, or similar personnel.

e. To persons working in shipyards whose duties do not require access to classified information.

f. To persons who can be prevented from accessing classified information by being escorted by cleared personnel.

g. To food service personnel, vendors and similar commercial sales or service personnel whose duties do not require access to classified information.

h. To maintenance or cleaning personnel who may only have inadvertent access to classified information unless such access cannot be reasonably prevented.

i. To persons who perform maintenance on office equipment, computers, typewriters, and similar equipment who can be denied classified access by physical security measures.

j. To perimeter security personnel who have no access to classified information.

k. To drivers, chauffeurs and food service personnel.

3-405 -- Dual Citizenship

Persons claiming both U.S. and foreign citizenship shall be processed: under paragraph 3-401, above, and adjudicated in accordance with the "Foreign Preference" standard in Appendix I.

3-406 -- One-Time Access

Circumstances may arise where an urgent operational or contractual exigency exists for cleared DoD personnel to have one-time or short duration access to classified information at a higher

level than is authorized by the existing security clearance. In many instances, the processing time required to upgrade the clearance would preclude timely access to the information. In such situations, and only for compelling reasons in furtherance of the DoD mission, an authority referred to in subparagraph a., below, may grant higher level access on a temporary basis subject to the terms and conditions prescribed below. This special authority may be revoked for abuse, inadequate record keeping, or inadequate security oversight. These procedures do not apply when circumstances exist which would permit the routine processing of an individual for the higher level clearance. Procedures and conditions for effecting emergency one-time access to the next higher classification level are as follows:

a. Authorization for such one-time access shall be granted by a flag or general officer, a general court martial convening authority or equivalent Senior Executive Service member, after coordination with appropriate security officials.

b. The recipient of the one-time access authorization must be a U.S. citizen, possess a current DoD security clearance, and the access required shall be limited to classified information one level higher than the current clearance.

c. Such access, once granted, shall be canceled promptly when no longer required, at the conclusion of the authorized period of access, or upon notification from the granting authority.

d. The employee to be afforded the higher level access shall have been continuously employed by a DoD Component or a cleared DoD contractor for the preceding 24-month period. Higher level access is not authorized for part-time employees.

e. Pertinent local records concerning the employee concerned shall be reviewed with favorable results.

f. Whenever possible, access shall be confined to a single instance or at most, a few occasions. The approval for access shall automatically expire 30 calendar days from date access commenced. If the need for access is expected to continue for a period in excess of 30 days, written approval of the granting authority is required. At such time as it is determined that the need for access is expected to extend beyond 90 days, the individual concerned shall be promptly processed for the level of clearance required. When extended access has been approved, such access shall be canceled at or before 90 days from original date of access.

g. Access at the higher level shall be limited to information under the control and custody of the authorizing official and shall be afforded under the general supervision of a properly cleared employee. The employee charged with providing such supervision shall be responsible for:

(1) recording the higher-level information actually revealed,
(2) the date(s) such access is afforded, and
(3) the daily retrieval of the material accessed.

h. Access at the next higher level shall not be authorized for COMSEC, SCI, NATO, or foreign government information.

i. The exercise of this provision shall be used sparingly and repeat use within any 12 month period on behalf of the same individual is prohibited. The approving authority shall maintain a record containing the following data with respect to each such access approved:

(1) The name, and SSN of the employee afforded higher level access.

(2) The level of access authorized.

(3) Justification for the access, to include an explanation of the compelling reason to grant the higher level access and specifically how the DoD mission would be furthered.

(4) An unclassified description of the specific information to which access was authorized and the duration of access along with the date(s) access was afforded.

(5) A listing of the local records reviewed and a statement that no significant adverse information concerning the employee is known to exist.

(6) The approving authority's signature certifying (1) through (5), above.

(7) Copies of any pertinent briefings/debriefings administered to the employee.

3-407 -- Access by Retired Flag and/or General Officers

a. Upon determination by an active duty flag/general officer that there are compelling reasons, in furtherance of the Department of Defense mission, to grant a retired flag/general officer access to classified information in connection with a specific DoD program or mission, for a period not greater than 90 days, the investigative requirements of this Regulation may be waived. The access shall be limited to classified information at a level commensurate with the security clearance held at the time of retirement -- not including access to SCI.

b. The flag/general officer approving issuance of the clearance shall, provide the appropriate DoD Component central clearance facility a written record to be incorporated into the DCII detailing:

(1) Full identifying data pertaining to the cleared subject;
(2) The classification of the information to which access was authorized.

c. Such access may be granted only after the compelling reason and the specific aspect of the DoD mission which is served by granting such access has been detailed and under the condition that the classified materials involved are not removed from the confines of a government installation or other area approved for storage of DoD classified information.

Section 5 -- Special Access Programs

3-500 -- General

It is the policy of the Department of Defense to establish, to the extent possible, uniform and consistent personnel security investigative requirements. Accordingly, investigations exceeding

established requirements are authorized only when mandated by statute, national regulations, or international agreement or Executive Order 12968 or its successor. In this connection, there are certain special access programs (SAPs) originating at the national or international level that require personnel security investigations and procedures of a special nature. Those programs and the special investigative requirements imposed by them are described in this section. A SAP is any program designed to control access, distribution, and protection of particularly sensitive information established pursuant to E.O. 12958 (reference (j)) and prior Executive orders. DoD Directive O-5205.7 (reference (qq)) prescribes policy and procedures for establishment, administration and reporting of Departmental SAPs.

3-501 -- Sensitive Compartmented Information (SCI)

a. The investigative requirements for access to SCI is an SBI (See paragraph 4, Appendix B) including a NAC on the individual's spouse or cohabitant. When conditions indicate, additional investigation shall be conducted on the spouse of the individual and members of the immediate family (or other persons to whom the individual is bound by affection or obligation) to the extent necessary to permit a determination by the adjudication agency that the Personnel Security standards of DCID 1/14 (reference (l)) are met.

b. A previous investigation conducted within the past five years which substantially meets the investigative requirements prescribed by this section may serve as a basis for granting access approval provided that there has been no break in the individual's military service, DoD civilian employment, or access to classified information under the Industrial Security Program greater than 24 months. The individual shall submit one copy of an updated PSQ covering the period since the completion of the last SBI and/or SSBI and certify any substantive changes that may have occurred.

c. In accordance with DCID 1/14 (reference (l)), a ***Top Secret*** security clearance shall not be a prerequisite for access to SCI. Determination of eligibility for access to SCI under reference (l) shall include eligibility for access to ***Top Secret*** and below.

3-502 -- Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI)

The investigative requirement for access to SIOP-ESI is an SBI, including a NAC on the spouse and the individual's immediate family who are 18 years of age or over and who are United States citizens other than by birth or who are resident aliens.

3-503 -- Presidential Support Activities

a. DoD Directive 5210.55 (reference (r)) prescribes the policies and procedures for the nomination, screening, selection, and continued evaluation of DoD military and civilian personnel and contractor employees assigned to or utilized in Presidential Support activities. The type of investigation of individuals assigned to Presidential Support activities varies according to whether the person investigated qualifies for Category One or Category Two as indicated below:

(1) ***Category One***

(a) Personnel assigned on a permanent or full-time basis to duties in direct support of the President (including the office staff of the Director, White House Military Office, and all individuals under his control):

1. Presidential air crew and associated maintenance and security personnel.

2. Personnel assigned to the White House communications activities and the Presidential retreat.

3. White House transportation personnel.

4. Presidential mess attendants and medical personnel.

5. Other individuals filling administrative positions at the White House.

(b) Personnel assigned on a temporary or part-time basis to duties supporting the President:

1. Military Social Aides.

2. Selected security, transportation, flight-line safety, and baggage personnel.

3. Others with similar duties.

(c) Personnel assigned to the Office of the Military Aide to the Vice President.

(2) ***Category Two***

(a) Personnel assigned to honor guards, ceremonial units, and military bands who perform at Presidential functions and facilities.

(b) Employees of contractors who provide services or contractors employees who require unescorted access to Presidential Support areas, activities, or equipment -- including maintenance of the Presidential retreat, communications, and aircraft.

(c) Individuals in designated units requiring a lesser degree of access to the President or Presidential Support activities.

b. Personnel nominated for Category One duties must have been the subject of an SBI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The SBI must have been completed within the 12 months preceding selection for Presidential Support duties. If such an individual marries subsequent to the completion of the SBI, the required spouse check shall be made at that time.

c. Personnel nominated for Category Two duties must have been the subject of a BI, including a NAC on the spouse and all members of the individual's immediate family of 18 years of age or over who are United States citizens other than by birth or who are resident aliens. The Bl must have been completed within the 12 months preceding selection for Presidential Support duties. It should be noted that duties (separate and distinct from their Presidential Support responsibilities)

of some Category Two personnel may make it necessary for them to have special access clearances which require an SBI.

d. The U.S. citizenship of foreign-born immediate family members of all Presidential Support nominees must be verified by investigation.

e. A limited number of Category One personnel having especially sensitive duties have been designated by the Director, White House Military Office as "Category A." These personnel shall be investigated under special scoping in accordance with the requirements of reference (jj).

3-504 -- Nuclear Weapon Personnel Reliability Program (PRP)

a. DoD Directive 5210.42 (reference(s)) sets forth the standards of individual reliability required for personnel performing duties associated with nuclear weapons and nuclear components. The investigative requirement for personnel performing such duties is:

(1) ***Critical Position:*** BI. In the event that it becomes necessary to consider an individual for a critical position and the required BI has not been completed, interim certification may be made under carefully controlled conditions as set forth below.

(a) The individual has had a favorable DNACI, NAC (or ENTNAC) within the past 5 years without a break in service or employment in excess of I year.

(b) The BI has been requested.

(c) All other requirements of the PRP screening process have been fulfilled.

(d) The individual is identified to supervisory personnel as being certified on an interim basis.

(e) The individual is not used in a two-man team with another such individual.

(f) Justification of the need for interim certification is documented by the certifying official.

(g) Should the BI not be completed within 150 days from the date of the request, the certifying official shall query the Component clearance authority, who shall ascertain from DIS the status of the investigation. On the basis of such information, the certifying official shall determine whether to continue or to withdraw the interim certification.

(2) ***Controlled Position: DNACI/NACI***

(a) An ENTNAC completed for the purpose of first term enlistment or induction into the Armed Forces does not satisfy this requirement.

(b) Interim certification is authorized for an individual who has not had a DNACI/NACI completed within the past 5 years, subject to the following conditions:

1. The individual has had a favorable ENTNAC/NAC, or higher investigation, that is more than 5 years old and has not had a break in service or employment in excess of 1 year.

2. A DNACI/NACI has been requested at the time of interim certification.

3. All other requirements of the PRP screening process have been fulfilled.

4. Should the DNACI/NACI not be completed within 90 days from the date of the request, the procedures set forth in a(l)(g), above, for ascertaining the delay of the investigation in the case of a critical position shall apply.

(3) ***Additional requirements apply.***

(a) The investigation upon which certification is based must have been completed within the last 5 years from the date of initial assignment to a PRP position and there must not have been a break in service or employment in excess of 1 year between completion of the investigation and initial assignment.

(b) In those cases in which the investigation was completed more than 5 years prior to initial assignment or in which there has been a break in service or employment in excess of I year subsequent to completion of the investigation, a reinvestigation is required.

(c) Subsequent to initial assignment to the PRP, reinvestigation is not required so long as the individual remains in the PRP

(d) A medical evaluation of the individual as set forth in DoD Directive 5210.42 (reference(s)).

(e) Review of the individual's personnel file and other official records and information locally available concerning behavior or conduct which is relevant to PRP standards.

(f) A personal interview with the individual for the purpose of informing him of the significance of the assignment, reliability standards, the need for reliable performance, and of ascertaining his attitude with respect to the PRP.

(g) Service in the Army, Navy and Air Force Reserve does not constitute active service for PRP purposes.

3-505 -- Access to North Atlantic Treaty Organization (NATO) Classified Information

a. Personnel assigned to a NATO staff Position requiring access to ***NATO Cosmic (Top Secret)s Secret or Confidential*** information shall have been the: subject of a favorably adjudicated BI (10 year scope), DNACI/NACI or NACI ENTNAC, current within five years prior to the assignment, in accordance with USSAN Instruction 1-69 (reference (kk)) and paragraph 3-705 below.

b. Personnel not assigned to a NATO staff position, but requiring access to ***NATO COSMIC, Secret or Confidential*** information in the normal course of their duties, must possess the equivalent final U.S. security clearance based upon the appropriate personnel security investigation (Appendix B) required by paragraph 3-401 and 3-709 of this Regulation.

3-506 -- Other Special Access Programs (SAPs)

Special investigative requirements for SAPs not provided for in this paragraph may be established only as part of the written program approval of the Deputy Secretary of Defense in accordance with the SAP approval process prescribed for in DoD Directive O-5205.7 (reference (qq)).

Section 6 -- Certain Positions Not Necessarily Requiring Access to Classified Information

3-600 -- General

DoD Directive 5200.8 (reference (t)) outlines the authority of military commanders under the Internal Security Act of 1950 to issue orders and regulations for the protection of property or places under their command. Essential to carrying out this responsibility is a commander's need to protect the command against the action of untrustworthy persons. Normally, the investigative requirements prescribed in this Regulation should suffice to enable a commander to determine the trustworthiness of individuals whose duties require access to classified information or appointment to positions that are sensitive and do not involve such access. However, there are certain categories of positions or duties which, although not requiring access to classified information, if performed by untrustworthy persons, could enable them to jeopardize the security of the command or otherwise endanger the national security. The investigative requirements for such positions or duties are detailed in this section.

3-601 -- Access to Restricted Areas, Sensitive Information or Equipment Not Involving Access to Classified Information

a. Access to restricted areas, sensitive information or equipment by DoD military, civilian or contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NAC (or ENTNAC) or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NAC shall be conducted and favorably reviewed by the appropriate component agency or activity prior to permitting such access. DoD Components shall not request, and shall not direct or permit their contractors to request, security clearances to permit access to areas when access to classified information is not required in the normal course of duties or which should be precluded by appropriate security measures. In determining trustworthiness under this paragraph, the provisions of paragraph 2-200 and Appendix I will be utilized.

b. In meeting the requirements of this paragraph, approval shall be obtained from one of the authorities designated in paragraph A, Appendix F of this Regulation, for authority to request NACs on DoD military, civilian or contractor employees. A justification shall accompany each request which shall detail the reasons why escorted access would not better serve the national

security. Requests for investigative requirements beyond a NAC shall be forwarded to the Deputy Under Secretary of Defense for Policy for approval.

c. ***NAC requests shall***

(1) be forwarded to DIS in accordance with the provisions of paragraph B, Appendix C,

(2) contain a reference to this paragraph on the DD Form 398-2, and

(3) list the authority in Appendix F who approved the request.

d. Determinations to deny access under the provisions of this paragraph must not be exercised in an arbitrary, capricious, or discriminatory manner and shall be the responsibility of the military or installation commander as provided for in DoD Directive 5200.8 (reference (t)).

3-602 -- Nonappropriated Fund Employees

Each Nonappropriated Fund employee who is employed in a position of trust as designated by an official authorized in paragraph H, Appendix F, shall have been the subject of a NAC completed no longer than 12 months prior to employment or a prior personnel security investigation with no break in Federal service or employment greater than 12 months in accordance with DoD Manual 1401.1-M, (reference (u)). An individual who does not meet established suitability requirements may not be employed without prior approval of the authorizing official. Issuance of a ***Confidential or Secret*** clearance will be based on a DNACI or NACI in accordance with paragraph 3-401.

3-603 -- Customs Inspectors

DoD employees appointed as customs inspectors, under waivers approved in accordance with DoD 5030.49-R (reference (v)), shall have undergone a favorably adjudicated NAC completed within the past 5 years unless there has been a break in DoD employment greater than 1 year in which case a current NAC is required.

3-604 -- Red Cross/United Service Organizations Personnel

A favorably adjudicated NAC shall be accomplished on Red Cross or United Service Organizations personnel as prerequisite for assignment with the Armed Forces overseas (DoD Directive 5210.25 (reference (w)).

3-605 -- Officials Authorized to Issue Security Clearances

Any person authorized to adjudicate personnel security clearances shall have been the subject of a favorably adjudicated BI.

3-606 -- Personnel Security Clearance adjudication Officials

Any person selected to serve with a board, committee, or other group responsible for adjudicating personnel security cases shall have been the subject of a favorably adjudicated BI.

3-607 -- Persons Requiring DoD Building Passes

Pursuant to DoD Directive 5210.46 (reference (z)), each person determined by the designated authorities of the Components concerned as having an official need for access to DoD buildings in the National Capital Region shall be the subject of a favorably, adjudicated NAC prior to issuance of a DoD building pass. Conduct of a BI for this purpose is prohibited unless approved in advance by ODUSD(P).

3-608 -- Foreign National Employees Overseas Not Requiring Access to Classified Information

Foreign nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of the following record checks, initiated by the appropriate military department investigative organization consistent with paragraph 2-404, prior to employment:

a. Host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and

b. DCII

c. FBI-HQ/ID (Where information exists regarding residence by the foreign national in the United States for one year or more since age 18)

3-609 -- Special Agents and Investigative Support Personnel

Special agents and those noninvestigative personnel assigned to investigative agencies whose official duties require continuous access to complete investigative files and material require an SBI.

3-610 -- Persons Requiring Access to Chemical Agents

Personnel whose duties involve access to or security of chemical agents shall be screened initially for suitability and reliability and shall be evaluated on a continuing basis at the supervisory level to ensure that they continue to meet the high standards required. At a minimum, all such personnel shall have had a favorably adjudicated NAC completed within the last 5 years prior to assignment in accordance with the provisions of DoD Directive 5210.65 (reference (y)).

3-611 -- Education and Orientation Personnel

Persons selected for duties in connection with programs involving the education and orientation of military personnel shall have been the subject of a favorably adjudicated NAC prior to such assignment. This does not include teachers/administrators associated with university extension courses conducted on military installations in the United States. Non-US citizens from a country listed in Appendix H shall be required to undergo a BI if they are employed in a position covered by this paragraph.

3-612 -- Contract Guards

Any person performing contract guard functions shall have been the subject of a favorably adjudicated NAC prior to such assignment.

3-613 -- Transportation of Arms, Ammunition and Explosives (AA&E)

Any DoD military, civilian or contract employee (including commercial carrier) operating a vehicle or providing security to a vehicle transporting Category I, II or ***Confidential*** AA&E shall have been the subject of a favorably adjudicated NAC or ENTNAC.

3-614 -- Personnel Occupying Information Systems Positions Designated ADP-I, ADP-II & ADP-III.

DoD military, civilian personnel, consultants, and contractor personnel performing on unclassified automated information systems may be assigned to one of three position sensitivity designations (in accordance with Appendix K) and investigated as follows:

ADP-I: BI

ADP-II: DNACI/NACI

ADP-III: NAC/ENTNAC

Those personnel falling in the above categories who require access to classified information will, of course, be subject to the appropriate investigative scope contained in paragraph 3-401, above.

3-615 -- Others

Requests for approval to conduct an investigation on other personnel, not provided for in paragraphs 3-601 through 3-614, above, considered to fall within the general provisions of paragraph 3-600 above, shall be submitted, detailing the justification therefor, for approval to the Deputy Under Secretary of Defense for Policy. Approval of such requests shall be contingent upon an assurance that appropriate review procedures exist and that adverse determinations will be made at no lower than major command level.

Section 7 -- Reinvestigation

3-700 -- General

DoD policy prohibits unauthorized and unnecessary investigations. There are, however, certain situations and requirements that necessitate reinvestigation of an individual who has already been investigated under the provisions of this Regulation. It is the policy to limit reinvestigation of individuals to the scope contained in paragraph 5, Appendix B to meet overall security requirements. Reinvestigation, generally, is authorized only as follows:

a. To prove or disprove an allegation relating to the criteria set forth in paragraph 2-200 of this Regulation with respect to an individual holding a security clearance or assigned to a position that requires a trustworthiness determination;

b. To meet the periodic reinvestigation requirements of this regulation with respect to those security programs enumerated below; and

c. Upon individual request, to assess the current eligibility of individuals who did not receive favorable adjudicative action after an initial investigation, if a potential clearance need exists and there are reasonable indications that the factors upon which the adverse determination was made no longer exists.

3-701 -- Allegations Related to Disqualification

Whenever questionable behavior patterns develop, derogatory information is discovered, or inconsistencies arise related to the disqualification criteria outlined in paragraph 2-200 that could have an adverse impact on an individual's security status, a Special Investigative Inquiry (SII), psychiatric, drug or alcohol evaluation, as appropriate, may be requested to resolve all relevant issues in doubt. If it is essential that additional relevant personal data is required from the investigative subject, and the subject fails to furnish the required data, the subject's existing security clearance or assignment to sensitive duties shall be terminated in accordance with paragraph 8-201 of this Regulation.

3-702 -- Access to Sensitive Compartmented Information (SCI)

Each individual having current access to SCI shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B.

3-703 -- Critical-sensitive Positions

Each DoD civilian employee occupying a critical sensitive position shall be the subject of a PR conducted an a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B.

3-704 -- Presidential Support Duties

Each individual assigned Presidential Support duties shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B.

3-705 -- NATO Staff

Each individual assigned to a NATO staff position requiring a COSMIC clearance shall be the subject of a PR conducted on a 5-year recurring basis scoped as set forth in paragraph 5, Appendix B. Those assigned to a NATO staff position requiring a NATO SECRET clearance shall be the subject of a new NAC conducted on a 5-year recurring basis.

3-706 -- Extraordinarily Sensitive Duties

In extremely limited instances, extraordinary national security implications associated with certain SCI duties may require very special compartmentation and other special security measures. In such instances, a Component SOIC may, with the approval of the Deputy Under Secretary of Defense for Policy, request PR's at intervals of less than 5 years as outlined in paragraph 5, Appendix B. Such requests shall include full justification and a recommendation as to the desired frequency. In reviewing such requests, the Deputy Under Secretary of Defense for Policy shall give due consideration to:

a. The potential damage that might result from the individual's defection or abduction.

b. The availability and probable effectiveness of means other than reinvestigation to evaluate factors concerning the individual's suitability for continued SCI access.

3-707 -- Foreign Nationals Employed by DoD Organizations Overseas

Foreign nationals employed by DoD organizations overseas who have been granted a "Limited Access Authorization" pursuant to paragraph 3-402 shall be the subject of a PR, as set forth in paragraph 5, Appendix B, conducted under the auspices of DIS by the appropriate military department or other U.S. Government investigative agency consistent with paragraph 2-404 and Appendix J of this Regulation.

3-708 -- Persons Accessing Very Sensitive Information Classified Secret

a. Heads of DoD Components shall submit a request to the Deputy Under Secretary of Defense for Policy for approval to conduct periodic reinvestigations on persons holding Secret clearances who are exposed to very sensitive Secret information.

b. Generally, the Deputy Under Secretary of Defense for Policy will only approve periodic reinvestigations of persons having access to Secret information if the unauthorized disclosure of the information in question could reasonably be expected to:

(l) Jeopardize human life or safety.

(2) Result in the loss of unique or uniquely productive intelligence sources or methods vital to U.S. security.

(3) Compromise technologies, plans, or procedures vital to the strategic advantage of the United States.

c. Each individual accessing very sensitive Secret information who has been designated by an authority listed in paragraph A, Appendix F as requiring periodic reinvestigation, shall be the subject of a PR conducted on a 5-year recurring basis scoped as stated in paragraph 5, Appendix B.

3-709 -- Access to Top Secret Information

Each individual having current access to Top Secret information shall be the subject of a PR conducted on a 5-year recurring basis scoped as outlined in paragraph 5, Appendix B.

3-710 -- Personnel Occupying Computer Positions Designated ADP-1

All DoD military, civilians, consultants, and contractor personnel occupying computer positions designated ADP-I, shall be the subject of a PR conducted on a 5-year recurring basis as set forth in paragraph 5, Appendix B.

Section 8 -- Authority to Waive Investigative Requirements

3-800 -- Authorized Officials

Only an official designated in paragraph G, Appendix F, is empowered to waive the investigative requirements for appointment to a sensitive position, assignment to sensitive duties or access to classified information pending completion of the investigation required by this chapter. Such waiver shall be based upon certification in writing by the designated official that such action is necessary to the accomplishment of a DoD mission. A minor investigative element that has not been met should not preclude favorable adjudication -- nor should this require a waiver when all other information developed on an individual during the course of a prescribed investigation is favorable.

Chapter V

Requesting Personnel Security Investigations

5-100 -- General

Requests for personnel security investigations shall be limited to those required to accomplish the Defense mission. Such requests shall be submitted only by the authorities designated in paragraph 5-101 below. These authorities shall be held responsible for determining if persons under their jurisdiction require a personnel security investigation. Proper planning must be effected to ensure that investigative requests are submitted sufficiently in advance to allow completion of the investigation before the time it is needed to grant the required clearance or otherwise make the necessary personnel security determination.

5-101 -- Authorized Requesters

Requests for personnel security investigation shall be accepted only from the requesters designated below:

a. ***Military Departments***

(1) ***Army***

(a) Central Clearance Facility.
(b) All activity commanders.
(c) Chiefs of recruiting stations.

(2) ***Navy*** (including Marine Corps)

(a) Central Adjudicative Facility

(b) Commanders and commanding officers of organizations listed on the Standard Navy Distribution List.

(c) Chiefs of recruiting stations.

(3) ***Air Force***

(a) Air Force Security Clearance Office.
(b) Assistant Chief of Staff for Intelligence.
(c) All activity commanders.
(d) Chiefs of recruiting stations.

b. ***Defense Agencies*** -- Directors of Security and activity commanders.

c. ***Organization of the Joint Chiefs of Staff*** -- Chief, Security Division.

d. ***Office of the Secretary of Defense*** -- Director for Personnel and Security, Washington Headquarters Services.

e. Commanders of Unified and Specified Commands or their designees.

f. Such other requesters approved by the Deputy Under Secretary of Defense for Policy.

5-102 -- Criteria for Requesting Investigations

Authorized requesters shall use the tables set forth in Appendix D to determine the type of investigation that shall be requested to meet the investigative requirement of the specific position or duty concerned.

5-103 -- Request Procedures

To insure efficient and effective completion of required investigations, all requests for personnel security investigations shall be prepared and forwarded in accordance with Appendix C and the investigative jurisdictional policies set forth in Section 4, Chapter II of this regulation.

5-104 -- Priority Requests

To insure that personnel security investigations are conducted in an orderly and efficient manner, requests for priority for individual investigations or categories of investigations shall be kept to a minimum. DIS shall not assign priority to any personnel security investigation or categories of investigations without written approval of the Deputy Under Secretary of Defense for Policy.

5-105 -- Personnel Data Provided by the Subject of the Investigation

a. To conduct the required investigation, it is necessary that the investigative agency be provided certain relevant data concerning the subject of the investigation. The Privacy Act of 1974 (reference (m)) requires that, to the greatest extent practicable, personal information shall be obtained directly from the subject individual when the information may result in adverse determinations affecting an individual's rights, benefits, and privileges under Federal programs.

b. Accordingly, it is incumbent upon the subject of each personnel security investigation to provide the personal information required by this Regulation. At a minimum, the individual shall complete the appropriate investigative forms, provide fingerprints of a quality acceptable to the FBI, and execute a signed release, as necessary, authorizing custodians of police, credit, education, employment, and medical and similar records, to provide relevant record information to the investigative agency. When the FBI returns a fingerprint card indicating that the quality of the fingerprints is not acceptable, an additional set of fingerprints will be obtained from the subject. In the event the FBI indicates that the additional fingerprints are also unacceptable, no further attempt to obtain more fingerprints need be made; this aspect of the investigation will then be processed on the basis of the name check of the FBI files. As an exception, a minimum of three attempts will be made (1) for all Presidential Support cases, (2) for SCI access nominations if the requester so indicates, and (3) in those cases in which more than minor derogatory information exists. Each subject of a personnel security investigation conducted under the provisions of this regulation shall be furnished a Privacy Act Statement advising of (1)

the authority for obtaining the personal data, (2) the principal purpose(s) for obtaining it, (3) the routine uses, (4) whether disclosure is mandatory or voluntary, (5) the effect on the individual if it is not provided, and (6) that subsequent use of the data may be employed as part of an aperiodic review process to evaluate continued eligibility for access to classified information.

c. Failure to respond within the time limit prescribed by the requesting organization with the required security forms or refusal to provide or permit access to the relevant information required by this Regulation shall result in termination of the individual's security clearance or assignment to sensitive duties utilizing the procedures of paragraph 8-201 or further administrative processing of the investigative request.

Chapter VI

Adjudication

6-100 -- General

a. The standard which must be met for clearance or assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interests of national security.

b. The principal objective of the DoD personnel security adjudicative function, consequently, is to assure selection of persons for sensitive positions who meet this standard. The adjudication process involves the effort to assess the probability of future behavior which could have an effect adverse to the national security. Since few, if any, situations allow for positive, conclusive evidence of certain future conduct, it is an attempt to judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security. It is invariably a subjective determination, considering the past but necessarily anticipating the future. Rarely is proof of trustworthiness and reliability or untrustworthiness and unreliability beyond all reasonable doubt.

c. Establishing relevancy is one of the key objectives of the personnel security adjudicative process in evaluating investigative material. It involves neither the judgment of criminal guilt nor the determination of general suitability for a given position; rather, it is the assessment of a; person's trustworthiness and fitness for a responsibility which could, if abused, have unacceptable consequences for the national security.

d. While equity demands optimal uniformity in evaluating individual cases, assuring fair and consistent assessment of circumstances from one situation to the next, each case must be weighed on its own merits, taking into consideration all relevant facts, and prior experience in similar cases. All information of record, both favorable and unfavorable, must be considered and assessed in terms of accuracy, completeness, relevance, seriousness, and overall significance. In all adjudications the protection of the national security shall be the paramount determinant.

6-101 -- Central Adjudication

a. To ensure uniform application of the requirement of this Regulation and to ensure that DoD personnel security determinations are effected consistent with existing statutes and Executive orders, the head of each Military Department and Defense Agencies shall establish a single Central Adjudication Facility for his/her component. The function of such facility shall be limited to evaluating personnel security investigations and making personnel security determinations. The chief of each Central Adjudication Facility shall have the authority to act on behalf of the head of the Component concerned with respect to personnel security

determinations. All information relevant to determining whether a person meets the appropriate personnel security standard prescribed by this Regulation shall be reviewed and evaluated by personnel security specialists specifically designated by the head of the Component concerned, or designee.

b. In view of the significance each adjudicative decision can have on a person's career and to ensure the maximum degree of fairness and equity in such actions, a minimum level of review shall be required for all clearance/access determinations related to the following categories of investigations.

(1) ***BI/SBI/PR/ENAC/SII:***

(a) ***Favorable:*** Completely favorable investigations shall be reviewed and approved by a adjudicative official in the civilian grade of GS-7/9 or the military rank of 0-3.

(b) ***Unfavorable:*** Investigations that are not completely favorable shall undergo at least two levels of review by adjudicative officials, the second of which must be at the civilian grade of GS-11/12 or the military rank of 0-4. When an unfavorable administrative action is contemplated under paragraph 8-201, the letter of intent (LOI) to deny or revoke must be approved and signed by an adjudicative official at the civilian grade of GS-13/14 or the military rank of 0-5. A final notification of unfavorable administrative action, subsequent to the issuance of the LOI, must be approved and signed at the civilian grade of GS-14/15 or the military rank of 0-6.

(2) ***NACI/DNACI/NAC/ENTNAC:***

(a) ***Favorable:*** A completely favorable investigation may be finally adjudicated after one level of review provided that the decision making authority is at the civilian grade of GS-5/7 or the military rank of 0-2.

(b) ***Unfavorable:*** Investigations that are not completely favorable must be reviewed by an adjudicative official in the civilian grade of GS-7/9 or the military rank of 0-3. When an unfavorable administrative action is contemplated under paragraph 8-201, the letter of intent to deny/revoke must be signed by an adjudicative official at the civilian grade of GS-11/12 or the military rank of 0-4. A final notification of unfavorable administrative action subsequent to the issuance of the LOI must be signed by an adjudicative official at the civilian grade of GS-13 or the military rank of 0-5 or above.

c. Exceptions to the above policy may only be granted by the Deputy Under Secretary of Defense for Policy.

6-102 -- Evaluation of Personnel Security Information

a. The criteria and adjudicative policy to be used in applying the principles at paragraph 6-100, above, are set forth in paragraph 2-200 and Appendix 1 of this Regulation. The ultimate consideration in making a favorable personnel security determination is whether such determination is clearly consistent with the interests of national security and shall be an overall

common sense evaluation based on all available information. Such a determination shall include consideration of the following factors:

(1) The nature and seriousness of the conduct;
(2) The circumstances surrounding the conduct;
(3) The frequency and recency of the conduct;
(4) The age of the individual;
(5) The voluntariness of participation; and
(6) The absence or presence of rehabilitation.

b. Detailed adjudication policy guidance to assist adjudicators in determining whether a person is eligible for access to classified information or assignment to sensitive duties is contained in Appendix I. Adjudication policy for access to SCI is contained in DCID 1/14.

6-103 -- Adjudicative Record

a. Each clearance/access determination, whether favorable or unfavorable, shall be entered into the Defense Central Security Index (DCSI), a sub-element of the Defense Central Index of Investigations (DCII). (Operational details regarding implementation of the DCSI shall be implemented in a forthcoming change to this Regulation).

b. The rationale underlying each unfavorable administrative action shall be reduced to writing and is subject to the provisions of DoD Directive 5400.7 (reference (aa)) and DoD Directive 5400.11 (reference (bb)).

Chapter VII

Issuing Clearance and Granting Access

7-100 -- General

a. The issuance of a personnel security clearance (as well as the function of determining that an individual is eligible for access to Special Access program information, or is suitable for assignment to sensitive duties or such other duties that require a trustworthiness determination) is a function distinct from that involving the granting of access to classified information. Clearance determinations are made on the merits of the individual case with respect to the subject's suitability for security clearance. Access determinations are made solely on the basis of the individual's need for access to classified information in order to perform official duties. Except for suspension of access pending final adjudication of a personnel security clearance, access may not be finally denied for cause without applying the provisions of paragraph 8-102.

b. Only the authorities designated in Paragraph A, Appendix F are authorized to grant, deny or revoke personnel security clearances or Special Access authorizations (other than SCI). Any commander or head of an organization may suspend access for cause when there exists information raising a serious question as to the individual's ability or intent to protect classified information, provided that the procedures set forth in paragraph 8-102 of this Regulation are complied with.

c. All commanders and heads of DoD organizations have the responsibility for determining those position functions in their jurisdiction that require access to classified information and the authority to grant access to incumbents of such positions who have been cleared under the provisions of this Regulation.

7-101 -- Issuing Clearance

a. Authorities designated in Paragraph A, Appendix F shall record the issuance, denial, or revocation of a personnel security clearance in the DCII (see paragraph 6-103, above). A record of the clearance issued shall also be recorded in an individual's personnel/security file or official personnel folder, as appropriate.

b. A personnel security clearance remains valid until

(1) the individual is separated from the Armed Forces,

(2) separated from DoD civilian employment,

(3) has no further official relationship with DoD,

(4) official action has been taken to deny, revoke or suspend the clearance or access, or

(5) regular access to the level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties.

If an individual resumes the original status of (1), (2), (3), or (5) above, no single break in the individual's relationship with DoD exists greater than 24 months, and/or the need for regular access to classified information at or below the previous level recurs, the appropriate clearance shall be reissued without further investigation or adjudication provided there has been no additional investigation or development of derogatory information.

c. Personnel security clearances of DoD military personnel shall be granted, denied, or revoked only by the designated authority of the parent Military Department. Issuance, reissuance, denial, or revocation of a personnel security clearance by any DoD Component concerning personnel who have been determined to be eligible for clearance by another component is expressly prohibited. Investigations conducted on Army, Navy, and Air Force personnel by DIS will be returned only to the parent service of the subject for adjudication regardless of the source of the original request. The adjudicative authority will be responsible for expeditiously transmitting the results of the clearance determination. As an exception, the employing DoD Component may issue an interim clearance to personnel under their administrative jurisdiction pending a final eligibility determination by the individual's parent Component. Whenever an employing DoD Component issues an interim clearance to an individual from another Component, written notice of the action shall be provided to the parent Component.

d. When an SSBI (or PR) for access to SCI is initiated on a military member, who is assigned to a Defense agency (except DIA), OSD staff, or the Joint Staff, DIS will return the completed investigation to the appropriate Military Department CAF, in accordance with subsection 7-101.c., above, for issuance (or reissuance) of the SCI eligibility. The CAF shall be responsible for expeditiously transmitting the results of the SCI eligibility determination to the requesting Defense agency. For military personnel assigned to the DIA, the completed investigation will be forwarded to the DIA for the SCI eligibility determination. The DIA will expeditiously transmit the results of the SCI eligibility determination to the appropriate Military Department CAF.

e. When the Defense Industrial Security Clearance Office (DISCO) initiates an SSBI (or PR) for access to SCI on a contractor employee, DIS will return the completed investigation to the appropriate CAF with SCI cognizance. Following a favorable SCI eligibility determination, the CAF will notify DISCO of the outcome. If the SCI eligibility is denied or revoked, the CAF will complete all appropriate due process and appeal procedures before forwarding the case and all relevant additional documentation to DISCO for appropriate action, to include referral to the Defense Office of Hearings and Appeals (DOHA) for possible action under DoD Directive 5220.6 (reference (c)).

f. The interim clearance shall be recorded in the DCII (paragraph 6-103, above) by the parent DoD Component in the same manner as a final clearance.

7-102 -- Granting Access

a. Access to classified information shall be granted to persons whose official duties require such access and who have the appropriate personnel security clearance. Access determinations (other than for Special Access programs) are not an adjudicative function relating to an individual's suitability for such access. Rather they are decisions made by the commander that access is officially required.

b. In the absence of derogatory information on the individual concerned, DoD commanders and organizational managers shall accept a personnel security clearance determination, issued by any DoD authority authorized by this Regulation to issue personnel security clearance, as the basis for granting access, when access is required, without requesting additional investigation or investigative files.

c. The access level of cleared individuals will, wherever possible, be entered into the Defense Clearance and Investigations Index (DCII), along with clearance eligibility. However, completion of the DCII Access field is required effective 1 October 1993 in all instances where the adjudicator is reasonably aware of the level of classified access associated with a personnel security investigation. Agencies are encouraged to start completing this field as soon as possible.

7-103 -- Administrative Withdrawal

As set forth in paragraph 7-101.b., above, the personnel security clearance and access eligibility must be withdrawn when the events described therein occur. When regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties, the previously authorized access eligibility level must be administratively downgraded or withdrawn, as appropriate.

Chapter IX

Continuing Security Responsibilities

Section 1 -- Evaluating Continued Security Eligibility

9-100 -- General

A personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty that any human being will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to assure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, the individual's supervisor and, to a large degree, the individual himself. Therefore, the heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process.

9-101 -- Management Responsibility

a. Commanders and heads of organizations shall insure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this Regulation) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

b. The heads of all DoD components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long term, job-related security problems.

9-102 -- Supervisory Responsibility

Security programs shall be established to insure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the

individual concerned to correct any personal problem which may have a bearing upon the individual's continued eligibility for access.

a. In conjunction with the submission of PRs stated in Section 7, Chapter III, and paragraph 5, Appendix B, supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's continued eligibility for access to classified information is omitted.

b. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package.

> "I am aware of no information of the type contained at Appendix E, DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information."

c. If the supervisor is aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

> "I am aware of information of the type contained in Appendix E. DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)."

9-103 -- Individual Responsibility

a. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

b. Moreover, individuals having access to classified information must report promptly to their security office:

(1) Any form of contact, intentional or otherwise, with a citizen of a designated country, (Appendix H) unless occurring as a function of one's official duties.

(2) Attempts by representatives or citizens of designated countries to cultivate friendships or to place one under obligation.

(3) Attempts by representatives or citizens of foreign countries to:

(a) Cultivate a friendship to the extent of placing one under obligation that they would not normally be able to reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value.

(b) Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.

(c) Coerce by blackmail, by threats against or promises of assistance to relatives living under foreign control, especially those living in a designated country.

(4) All personal foreign travel in advance.

(5) Any information of the type referred to in paragraph 2-200 or Appendix I.

9-104 -- Co-worker Responsibility

Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

Section 2 -- Security Education

9-200 -- General

The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, heads of DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

9-201 -- Initial Briefing

a. All persons cleared for access to classified information or assigned to duties requiring a trustworthiness determination under this Regulation shall be given an initial security briefing. The briefing shall be in accordance with the requirements of paragraph 10-102, DoD 5200.1-R (reference (q)) and consist of the following elements:

(1) The specific security requirements of their particular job.

(2) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

(3) The prohibition against disclosing classified information, by any means, to unauthorized persons or discussing or handling classified information in a manner that would make it accessible to unauthorized persons.

(4) The penalties that may be imposed for security violations.

b. If an individual declines to execute Standard Form 189, **"Classified Information Nondisclosure Agreement,"** the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph 8-201, above.

9-202 -- Refresher Briefing

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in paragraph 10-101, DoD 5200.1-R (reference (q)) shall be tailored to fit the needs of experienced personnel.

9-203 -- Foreign Travel Briefing

a. DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security officer all personal foreign travel in advance of the travel being performed. When travel patterns, or the failure to report such travel, indicate the need for investigation, the matter will be referred to the appropriate counter-intelligence investigative agency.

b. Personnel having access to classified information shall be given a Foreign Travel Briefing by a counter-intelligence agent, security specialist, security manager, or other qualified individual, as a defensive measure prior to travel to a designated country (Appendix H) in order to alert them to their possible exploitation by hostile intelligence services. These personnel will also be debriefed upon their return. The briefings will be administered under the following conditions:

(1) Travel to or through a designated country for any purpose.

(2) Attendance at international, scientific, technical, engineering, or other professional meetings in the United States or in any country outside the United States when it can be anticipated that representative(s) of designated countries will participate or be in attendance.

c. Individuals who travel frequently, or attend or host meetings of foreign visitors as described in b.2., above, need not be briefed for each occasion, but shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

d. Records on such employees will be maintained for 5 years.

9-204 -- Termination Briefing

a. Upon termination of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

(1) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD Regulations applicable to the safeguarding of

classified information to which the individual has had access, and understands the implications thereof.

(2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession.

(3) An acknowledgment that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

(4) An acknowledgment that the individual will report without delay to the FBI or the DoD Component concerned any attempt by any unauthorized person to solicit classified information.

b. When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service who shall assure that it is recorded in the Defense Central Index of Investigations.

c. The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

d. In addition to the provisions of subparagraphs a., b., and c. above, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS-16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.

Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)

This directive was approved by the DCI July 2, 1998 as Director of Central Intelligence Directive 1/14 (DCID 1/14). It superseded DCID 1/14, as amended 12 August 1994. Annex F was added on October 13, 1999. At that time, some DCID numbers were modified and DCID 1/14 became DCID 6/4.

A complete copy of DCID 6/4 now consists of the basic DCID and Annexes A through F, as follows:

- Annex A - Investigative Standards for Background Investigations for Access to Classified Information.
- Annex B - Quality Control Guidelines for the Single Scope Background Investigation.
- Annex C - Adjudication Guidelines for Determining Eligibility for Access to Classified Information.
- Annex D - Appeals Procedures: Denial or Revocation of Access.
- Annex E - Standards for SCI Security Awareness Programs in the US Intelligence Community.
- Annex F: Reciprocity of SCI Eligibility Determinations

The President approved the Adjudicative Guidelines, Temporary Eligibility Standards and Investigative Standards required by Executive Order 12968 on March 24, 1997. This revised DCID incorporates the President's policy documents verbatim, at Annexes A and C, to promote the use of these common and consistent standards for government-wide security background investigations. These two annexes should be read in the context of the Director of Central Intelligence (DCI) special authorities, governing access eligibility to SCI, although the actual wording addresses a broader application to clearance actions.

The DCI exercises authority derived from statute and executive order over access eligibility to SCI and delegates this authority to Determination Authorities through Senior Officials of the Intelligence Community. (See Definitions.) Nothing in this directive or its annexes shall be deemed to preclude the DCI or the DDCI under the authority of the National Security Act of 1947, as amended, from taking any actions regarding an individual's SCI access.

Pursuant to the provisions of the National Security Act of 1947, as amended, and Executive Orders 12333 and 12968, the following personnel security guidelines, procedures, standards, and continuing security programs are hereby established for all US Government civilian and military personnel, consultants, contractors, employees of contractors, and other individuals who require access to SCI. Individual departments and agencies may establish such additional security steps as may be deemed necessary and appropriate to resolve issues and/or address employment standards unique to them to ensure that effective security is maintained.

1. Definitions.

a. Cohabitant--A person living in a spouse-like relationship with the individual requiring SCI information.

b. Compelling Need--A signed determination by a Senior Official of the Intelligence Community (SOIC) or his/her designee that the services of an individual are deemed essential to operation or mission

accomplishment.

c. Risk Assessment--A written evaluation supporting the adjudicative process, especially when a significant exception to a Personnel Security Standard is being considered. This assessment should consist of an evaluation from security, counterintelligence, and other technical or management experts as appropriate, and should contrast the compelling national security benefit of an individual accessed to SCI with the risk.

d. Determination Authority --A designee of a SOIC with responsibility for decisions rendered with respect to SCI access eligibility or ineligibility.

e. Immediate Family --The spouse, parents, siblings, children, and cohabitant of the individual requiring SCI access.

f. Intelligence Community --Those US Government organizations and activities identified in the National Security Act of 1947, as amended, 50 USC 401a(4), EO 12333, or successor orders, as making up such a Community.

g. Senior Officials of the Intelligence Community (SOICs) --The heads of organizations or activities within the Intelligence Community, as defined by the National Security Act of 1947, as amended, 50 USC 401a(4), and EO 12333.

h. Sensitive Compartmented Information --Classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the DCI.

2. Purpose.

The purpose of this directive is to enhance the security protection of SCI through the application of personnel security standards, procedures, and continuing security programs.

3. Applicability.

The provisions of this directive will apply to all persons (other than elected officials of the US Government, to include elected State Governors as may be required on an individual basis, Federal judges, and those individuals for whom the DCI makes a specific exception) without regard to a civilian or military status, form of employment, official rank or position, or length of service. This directive does not apply to situations involving the duly authorized disclosure of SCI to representatives of foreign governments and international organizations.

4. General.

a. The granting of access to SCI will be controlled under the strictest application of the "need-to-know" principle and in accordance with the personnel security standards and procedures set forth in this directive.

b. In accordance with DCID 1/19, "Security Policy for Sensitive Compartmented Information," and its supplement, "DCID 1/19 Security Policy Manual," those approved for access to SCI are required to sign a DCI-authorized nondisclosure agreement that includes a provision for prepublication review as a condition of access to SCI.

5. Personnel Security Standards.

Criteria for security approval of an individual on a need-to-know basis for access to SCI are as follows:

a. The individual requiring access to SCI must be a US citizen.

b. The individual's immediate family must also be US citizens.

c. Members of the individual's immediate family and any other persons to whom he or she is bound by affection or obligation should neither be subject to physical, mental, or other forms of duress by a foreign power or by persons who may be or have been engaged in criminal activity, nor advocate the use of force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means.

d. The individual must be stable; trustworthy; reliable; of excellent character, judgment, and discretion; and of unquestioned loyalty to the United States.

6. Exceptions to Personnel Security Standards.

Any exception to the Personnel Security Standards will be a common sense determination based on the fact that the available information supports a finding that the specific risk to national security is manageable in the specific case for which the exception is granted. The organization determining that an exception is warranted will document their finding in the individual's security record. As appropriate, a risk assessment, normally directed by the Determination Authority, may be required to aid in the determination of the appropriateness of granting an exception to one of the Personnel Security Standards. If accomplished, this assessment should become a part of the individual's security record.

a. The DCI is the exclusive authority for granting an exception to the requirement that the Subject be a US citizen.

b. The affected SOIC or specified designee may grant exception to the standard requiring US citizenship for the family members of an individual proposed for SCI access, as well as the standard requiring individuals to which Subject is bound by affection or obligation be free of any form of duress.

c. Exceptions to the US citizenship requirement for individuals to be accessed to SCI and their immediate family members shall require certification of a compelling need. This exception should be based upon a specific national security requirement and a certification of compelling need.

7. Investigative Requirements and Standards.

a. The investigation conducted on an individual under consideration for access to SCI will conform to the requirements of a Single Scope Background Investigation (SSBI) as defined in Annex A, "Investigative Standards for Background Investigations for Access to Classified Information." Quality Control procedures relevant to investigations are defined in Annex B, "Quality Control Guidelines for the Single Scope Background Investigation."

b. When conditions indicate, investigation of immediate family members will be conducted to the extent necessary to permit a determination by the adjudicating agency that the provisions of paragraph 5 of this directive are met.

c. Where a previous investigation has been conducted within the past five years that meets the

standards of Annex A, it will serve as a basis for granting access approval except where there is substantial information indicating that the employee may not satisfy the adjudicative guidelines in Annex C. If a previous investigation does not meet the Annex A standards, if it is more than five years old, or if there is a break in SCI access of two years or more, a current investigation will be required but may be limited to that necessary to bring the individual's file up-to-date in accordance with the investigative requirements set forth in Annex A of this directive, paragraphs 6 and 10. The up-dating process may be limited to review of applicable records, starting with an updated SF-86, and involve reinvestigation only when it appears the person may no longer satisfy standards for access under this directive. Should new information be developed during the current investigation that bears unfavorably on the individual's activities covered by the previous investigation, the current inquiries will be expanded as necessary to develop full details of this information.

d. Programs will be instituted requiring the periodic reinvestigation (PR) of personnel provided access to SCI. These SSBI-PRs will be conducted in accordance with the procedures and scope contained in the section of Annex A defining the SSBI-PR. The SSBI-PR may be expanded as necessary to resolve outstanding issues.

e. Notwithstanding the status of an individual's background investigation, departments and agencies with policies sanctioning the use of the polygraph for personnel security purposes may require polygraph examinations when deemed necessary by the department or agency head to be in the national security interest of the United States. Where they exist, such polygraph programs shall be characterized by unified training and certification as well as by coordination of scope, applicability and fairness issues to promote consistency, reciprocity and due process.

f. In those cases in which the individual has lived outside of the United States for a substantial period, a thorough assessment of the adequacy of the investigation in terms of fulfillment of the investigative requirements and judicious review of the information therein must be made before an exception is considered.

8. Temporary Eligibility for Access to SCI.

a. In exceptional cases, including national emergency situations and hostilities involving US personnel, the SOIC or his designee may determine that it is necessary or advisable in the national interest to authorize temporary access to SCI before completion of the SSBI. In this situation, the procedures contained in the Annex A section entitled "Investigative Standards for Temporary Eligibility for Access" will be complied with before temporary access is permitted. A personal interview of the individual by trained security, investigative, or counterintelligence personnel will be conducted wherever possible and practicable.

b. The SSBI and final evaluation will be completed at the earliest practicable moment unless an exception is granted by the DCI. Temporary eligibility for access is valid only at the agency granting it and other agencies which expressly agree to accept it and acknowledge understanding of its investigative basis. Therefore, certification to other organizations of individuals authorized temporary access will include explicit notification of the fact.

c. Temporary eligibility for access may be granted only to SCI necessary for the individual to perform authorized functions. Therefore, indoctrination briefings will be modified to the basic information

necessary to ensure protection of the SCI to which the individual will be exposed, and appropriate nondisclosure agreements signed.

9. Reporting Requirements.

Individuals who hold SCI access have special responsibilities and obligations to report to their cognizant security officer, in writing and when feasible in advance, activities, conduct or employment that could conflict with their ability to protect classified information from unauthorized disclosure or counterintelligence threats. A more detailed explanation and a listing of an individual's responsibilities and reporting requirements are contained in Annex E. In addition, initial and updated security documents (e.g. Statement of Personal History, Questionnaire for National Security Positions, Security Clearance Application) and security records shall include details of such employment, activities, associations and/or conduct to facilitate appropriate investigation and evaluation to determine whether the circumstances create an unacceptable risk to the security of SCI or of unauthorized disclosure. Annex C, Guideline L, "Outside Activities," summarizes the concern.

10. Determinations of Access Eligibility.

The evaluation of the information developed by investigation of an individual's loyalty and suitability will be accomplished by trained professional adjudicators under the cognizance of the SOIC concerned. When all other information developed on an individual is favorable, a minor investigative requirement that has not been met should not preclude a favorable access determination by an authorized adjudicative authority. In all evaluations, the protection of the national security is paramount. Any doubt concerning personnel having access to SCI should be resolved in favor of the national security, and the access should be denied or revoked. The ultimate determination of whether the granting of access is clearly consistent with the interest of national security will be an overall common sense determination based on all available information. The adjudicative guidelines for determining eligibility for access to SCI are contained in Annex C.

11. Appeals Procedures.

Annex D prescribes common appeals procedures to be followed when an individual's SCI access has been denied or revoked.

12. Continuing Security Programs.

a. To facilitate attainment of appropriate standards of personnel security and to augment both the access approval criteria and the investigative requirements established by this directive, member departments and agencies shall institute continuing security programs based on risk management principles for all individuals having access to SCI. In addition to security indoctrinations (see Annex E, "Standards for SCI Security Awareness Programs in the US Intelligence Community"), these programs will be tailored to create mutually supporting procedures to identify and resolve issues which bring into question an individual's loyalty and integrity or suggest the possibility of his or her being subject to undue influence or duress through foreign relationships or exploitable personal conduct. These programs should include the capacity for member departments and agencies to monitor the individual’s performance in a tailored program against the eligibility criteria and adjudicative standards when unresolved concerns are present. When an individual is assigned to perform sensitive work requiring access to SCI, the SOIC for the department, agency, or government program to which the individual is

assigned will assume security supervision of that individual throughout the period of his or her assignment.

b. The continuing security programs will include the following:

(1) Individuals are required to inform the department or agency that grants their SCI access about any personal problem or situation that may have a possible bearing on their eligibility for continued access to SCI and to seek appropriate guidance and assistance. Security guidance should be provided by an official who understands both the eligibility issues involved, and the unique sensitivities of the specific SCI program being supported. As appropriate, tailored monitoring programs should be established to ensure that individuals actively resolve problems which have led to concern about their continued eligibility for access. An individual participating in a monitoring program with a particular department or agency does not meet the criteria for automatic reciprocal acceptance of SCI eligibility as established by Executive Order 12968. In these situations, each organization should make their own determination of eligibility.

(2) SCI security education programs of the member departments and agencies will be established and maintained pursuant to the requirements of Annex E of this directive.

(3) Security awareness programs for supervisory personnel will be established and maintained to ensure that supervisory personnel recognize and discharge their special responsibility to safeguard SCI, including the need to assess continued eligibility for SCI access. These programs will provide practical guidance on indicators that may signal matters of security concern. Specific instructions concerning reporting procedures will be disseminated to enable the appropriate authority to take timely corrective action to safeguard the security of the United States as well as to provide all necessary help to the individual concerned to neutralize his or her vulnerability.

(4) Security review programs will ensure that appropriate security authorities always receive and exchange, in a timely manner, all information, including lead information, bearing on the security posture of persons having access to SCI. Personal history information will be kept current. Security and related files will be kept under continuing review.

(5) Where permitted by agency policy, security review programs may include the use of polygraph examinations conducted by a qualified polygraph examiner.

c. Whenever adverse or derogatory information is discovered or inconsistencies arise that could impact on an individual's security status, appropriate investigation will be conducted on a timely basis. The investigation will be of sufficient scope necessary to resolve the specific adverse or derogatory information or inconsistency in question so that a determination can be made as to whether the individual's continued utilization in activities requiring SCI is clearly consistent with the interest of national security.

13. Implementation.

Existing directives, regulations, agreements, and other guidance governing access to SCI as defined herein will be revised accordingly.

George J. Tennet — July 2, 1998

Director of Central Intelligence — Date

ANNEX A: Investigative Standards for Background Investigations for Access to Classified Information

(Note: The content of this Annex is taken verbatim from the Presidentially approved Investigative Standards and Temporary Eligibility Standards and should be read in the context of access eligibility to SCI, although the actual wording addresses a broader application to clearance actions.)

1. Introduction.

The following investigative standards are established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs), and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

2. The Three Standards.

There are three standards (Table 1 in the Appendix summarizes when to use each one):

a. The investigation and reinvestigation standards for "L" access authorizations and for access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by sect. 4.4 of Executive Order 12958);

b. The investigation standard for "Q" access authorizations and for access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

c. The reinvestigation standard for continued access to the levels listed in para. 2(b).

3. Exception to Periods of Coverage.

Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the Subject's eighteenth birthday to the present or to two years, whichever is longer.

4. Expanding Investigations.

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

5. Transferability.

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements of all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

6. Breaks in Service.

If a person who requires access has been retired or separated from US Government employment for less than two years and is the Subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (see Table 2).

7. The National Agency Check.

The National Agency Check is part of all investigations and reinvestigations. It consists of a review of:

a. Investigative and criminal history files of the FBI, including a technical fingerprint search;

b. OPM's Security/Suitability Investigations Index;

c. DoD's Defense Clearance and Investigations Index; and

d. Such other national agencies (e.g., CIA, INS) as appropriate to the individual's background.

STANDARD A
National Agency Check with Local Agency Checks and Credit Check (NACLC)

8. Applicability.

Standard A applies to investigations and reinvestigations for:

a. Access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by sect. 4.4 of Executive Order 12958), and

b. "L" access authorizations.

9. For Reinvestigations: When to Reinvestigate.

The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation, including when there has been a break in service.)

10. Investigative Requirements.

Investigative requirements are as follows:

a. Completion of forms: completion of Standard Form 86, including applicable releases and supporting documentation.

b. National Agency Check: completion of a National Agency Check.

c. Financial Review: verification of the Subject's financial status, including credit bureau checks covering all locations where the Subject has resided, been employed, or attended school for six months or more for the past seven years.

d. Date and Place of Birth: corroboration of date and place of birth through a check of appropriate documentation, if *not* completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

e. Local Agency Checks: as a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the Subject has lived, worked, and/or attended school within the last five years, and if applicable, of the appropriate agency for any identified arrests.

11. Expanding the Investigation.

The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

STANDARD B
Single Scope Background Investigation (SSBI)

12. Applicability.

Standard B applies to initial investigations for:

a. Access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

b. "Q" access authorizations.

13. Investigative Requirements.

Investigative requirements are as follows:

a. Completion of Forms: completion of Standard Form 86, including applicable releases and supporting documentation.

b. National Agency Check: completion of a National Agency Check.

c. National Agency Check for the Spouse or Cohabitant (if applicable): completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant.

d. Date and Place of Birth: corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

e. Citizenship: for individuals born outside the United States, verification of US citizenship directly from the appropriate registration authority; verification of US citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

f. Education: corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the Subject during the most recent three years.

g. Employment: verification of all employments for the past seven years; personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military service, including discharge type. For military members, all service within one

branch of the armed forces will be considered as one employment, regardless of assignments.

h. References: four references, of whom at least two are developed; to the extent practicable, all should have social knowledge of the Subject and collectively span at least the last seven years.

i. Former Spouse: an interview of any former spouse divorced within the last ten years.

j. Neighborhoods: confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

k. Financial Review: verification of the Subject's financial status, including credit bureau checks covering all locations where Subject has resided, been employed, and/or attended school for six months or more for the last seven years.

l. Local Agency Checks: a check of appropriate criminal history records covering all locations where, for the last ten years, the Subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (NOTE: If no residence, employment or education exceeds six months, local agency checks should be performed as deemed appropriate.)

m. Public Records: verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the Subject.

n. Subject Interview: a Subject Interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional Subject Interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

o. Polygraph (only agencies with approved personnel security polygraph programs): in departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

14. Expanding the Investigation.

The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professional, and law enforcement professionals may be conducted.

STANDARD C
Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)

15. Applicability.

Standard C applies to reinvestigations for:

a. Access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

b. "Q" access authorizations.

16. When to Reinvestigate.

The reinvestigation may be initiated at any time following completion of, but not later than five years

from date of, the previous investigation (see Table 2).

17. Reinvestigative Requirements.

Reinvestigative requirements are as follows:

a. Completion of Forms: completion of Standard Form 86, including applicable releases and supporting documentation.

b. National Agency Check: completion of a National Agency Check (fingerprint cards are required *only* if there has not been a previous valid technical check of the FBI).

c. National Agency Check for the Spouse or Cohabitant (if applicable): completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is *not* required if already completed in conjunction with a previous investigation or reinvestigation.

d. Employment: verification of all employments since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employments of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

e. References: interviews with two character references who are knowledgeable of the Subject; at least one will be a developed reference. To the extent practical, both should have social knowledge of the Subject and collectively span the entire period of the investigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

f. Neighborhoods: interviews of two neighbors in the vicinity of the Subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

g. Financial Review:

(1) Financial Status: verification of the Subject's financial status, including credit bureau checks covering all locations where Subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) Check of Treasury's Financial Database: Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated databases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

h. Local Agency Checks: a check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the Subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (NOTE: If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.)

i. Former Spouse: an interview with any former spouse unless the divorce took place before the date

of the last investigation or reinvestigation.

j. Public Records: verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the Subject since the date of the last investigation.

k. Subject Interviews: a Subject Interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional Subject Interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

18. Expanding the Reinvestigation.

The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

Appendix
Decision Tables

TABLE 1: WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investigation required is	Using standard
CONFIDENTIAL, SECRET, "L"	none ——— CONF,SEC,"L"	none ——— out of date NACLC or SSBI	NACLC	A
TOP SECRET, CSI; "Q"	none, CONF, SEC, "L" ——— TS, SCI; "Q"	none or current or out of date NACLC ——— out of date SSBI	SSBI ——— SSBI-PR	B ——— C

TABLE 2: REINVESTIGATION REQUIREMENTS

If requirement is for	And age of the investigation is	Type required if there has been a break in service of ____ months	
		0-23 months	24 months or more
CONFIDENTIAL	0 to 14 yrs. 11 mos. ——— 15 yrs. or more	none (NOTE1) ——— NACLC	NACLC
SECRET, "L"	0 to 9 yrs. 11 mos. ——— 10 yrs. or more	none (NOTE1) ——— NACLC	

TOP SECRET, SCI, "Q"	0 to 4 yrs. 11 mos. _____ 5 yrs. or more	none (NOTE1) _____ SSBI-PR	SSBI

NOTE 1: As a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation (NACLC or SSBI-PR) is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968.

Investigative Standards for Temporary Eligibility for Access

1. Introduction.

The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, "Access to Classified Information", are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

2. Temporary Eligibility for Access.

Based on a justified need meeting the requirements of section 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

3. Temporary Eligibility for Access at the CONFIDENTIAL and SECRET Levels and Temporary Eligibility for "L" Access Authorization.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).

4. Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization: For Someone who is the Subject of a Favorable Investigation not Meeting the Investigative Standards for Access at those Levels.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for a Single Scope Background Investigation (SSBI).

5. Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization: For Someone who is not the Subject of a current, favorable personnel or Personnel Security Investigation of any kind.

As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any

applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited SSBI, and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

6. Additional Requirements by Agencies.

Temporary eligibility for access must satisfy these minimum investigations standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968. Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968, "Access to Classified Information."

ANNEX B: Quality Control Guidelines for the Single Scope Background Investigation

1. Guidelines.

In accordance with the requirements of DCID 6/4 , this document sets out guidelines to maintain quality standards for the Single Scope Background Investigation (SSBI). These guidelines assume the adjudicator's perspective because the adjudicator is the ultimate customer for the SSBI. The guidelines are divided into:

- Definition of Quality
- Conduct of the Interview
- Collection Requirements (Coverage)
- Quality Control Activities.

SOICs will ensure that investigative personnel employed by or assigned or detailed to their agencies/departments receive adequate initial and ongoing training in investigation and interrogation techniques, as well as familiarization with counterintelligence issues that may arise during investigation. Training should also incorporate findings of contemporary research in personnel security and medical disciplines and, in addition, evolving legal issues that may impact investigation collection requirements. As much as possible, training should be conducted as a joint effort with other investigative entities supporting the Intelligence Community, to facilitate information sharing and to enhance reciprocity.

2. Definition of Quality.

A quality investigation is a thorough and comprehensive collection of favorable and unfavorable information from a variety of sources, past and present, that may include employment(s), reference(s), neighborhood(s), credit, police, and the Subject.

The determination of eligibility for access to sensitive compartmented information is a discretionary determination using the whole person concept that such access is clearly in the interests of the national security. Accordingly, the investigation will be comprehensive and in such detail so as to affirmatively address unquestioned loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling and protection of sensitive compartmented information.

3. Conduct of the Interview

The quality of the investigation depends on the investigator's ability to elicit information from a source knowledgeable about the Subject. This is basic to the conduct of any interview. The investigator should plan and execute each interview so as to obtain the maximum amount of information from a source. Available sources should be selected from each area of coverage to ensure that pertinent information about the Subject's entire background is developed.

The investigator should conduct the interview in person and find a suitable location that protects privacy. Telephonic interviews are strongly discouraged; however, occasionally exigent circumstances may dictate that the interviews be conducted by telephone. If a telephonic interview is necessary, the report

should always state why the interview was not conducted in person.

The investigator should initially advise the source of the reason/purpose for the investigation and should attempt to establish a degree of confidence in the source(s) that will promote a high level of rapport and cooperation.

The investigator should also advise the source about the Privacy Act of 1974, before completing the interview, since the source needs to understand that the Subject of the investigation has the right to review information provided by a source and has the right to know a source's identity, unless the source requests confidentiality.

4. Collection Requirement (Coverage)

a. For all Sources.

Investigators should establish the duration and nature of association between the source and the Subject to assess the source’s extent of knowledge. The investigator should always secure the source's full name and any other appropriate identifying data, particularly in the case of a source with a common name. All derogatory or noteworthy information concerning the Subject of the investigation that is provided by a source should be fully explored in the interview, including elicitation of the names of any corroborating sources or record information that will substantiate any derogatory testimony provided by the source. For all sources, the report should indicate what issue areas were covered and whether the information provided was favorable or unfavorable.

b. For References and Neighbors.

Depending on the source's degree of association, investigators should ask each reference or neighbor relevant information regarding the Subject's:

(1) Family, citizenship, education, employment, residence history, and military service.

(2) Reputation, character, honesty, trustworthiness, integrity, discretion, reliability, and temperament.

(3) Financial stability, organizational affiliations, and whether there is a history of mental, emotional, or physical health problems.

(4) Whether the Subject exhibits a pattern of excessive use of alcohol or has ever used illegal drugs or abused prescription drugs.

(5) Activities which indicate a lack of discretion or demonstrate poor judgment, a character flaw, or a personality disorder.

(6) Participation in criminal activity or an altercation with law enforcement agencies.

(7) Travels abroad for business or pleasure and degree of contact with foreign nationals.

(8) Unquestioned loyalty to the United States.

If a Subject has had access to classified information and a source is in a position to know, the investigator should ask whether the Subject properly handles classified information or has ever had a security violation. Finally, the investigator should ask if the source can recommend the Subject for a position of

trust and responsibility with the US Government or, in the case of a contractor, can the Subject be trusted with classified information. The investigator should conclude the interview by asking the source to provide names of additional references.

c. Follow-up Questions.

If a source provides noteworthy or derogatory information to questions in any of the above areas of consideration, the investigator should ask follow-up questions as necessary to elicit all available information. The investigator should report as fully as possible:

(1) The nature, extent, and seriousness of the conduct.

(2) The motivation for and the circumstances surrounding the conduct.

(3) The frequency and recency of the conduct.

(4) The Subject's age and maturity at the time of the conduct.

(5) Whether the conduct was voluntary or whether there was pressure, coercion, or exploitation leading to the conduct.

(6) Whether the Subject has been rehabilitated or has exhibited other pertinent behavioral changes since the conduct.

If the Subject has ended the questionable conduct, the investigator should attempt to determine the motivation for positive change. The investigator should also attempt to establish whether there may be personal animosity or bias towards the Subject on the part of the source(s). The investigator should supply any available documentary evidence relating to the conduct in addition to the report of the source.

d. For Employment References.

The investigator should identify and interview the best source(s) available. These employment references should include, but are not limited to, the Subject's immediate supervisor, coworker(s), and other persons with frequent professional contact. Where appropriate, the investigator should pursue the same line of inquiry as with references and neighbors. In particular, the investigator should inquire regarding:

(1) Whether the Subject is willing to abide by company policies and regulations.

(2) Whether the Subject appropriately safeguards the employer's proprietary/sensitive information.

(3) Whether the Subject is financially stable.

(4) Whether the Subject has a history of substance abuse, to include alcohol, and/or prescription drugs.

(5) Whether the Subject has been involved in any criminal activity.

(6) Whether the Subject is reliable and eligible for re-hire.

The investigator should obtain any available documentary evidence to support the report of the source(s).

e. For Subject Interviews.

The Subject is the best source of information about himself/herself. Hence, the investigator should explore with the Subject the same line of inquiry she/he pursues with a reference, neighborhood, and employment source(s). The investigator should obtain the Subject's version of the details surrounding all issues arising either in the course of the interview or in other parts of the investigation that have been completed by the time of the Subject Interview and report them completely. The investigator should inquire regarding:

(1) What happened and why.

(2) Where, when, how, and how often it happened.

(3) Who else was involved.

(4) Was the conduct voluntary.

Of particular value to the adjudicator is evidence that the Subject is being contradictory or dissembling. If the Subject claims to have ended the conduct, the investigator should attempt to determine the motivation for positive change. The investigator should report only the facts.

5. Quality Control Activities.

Quality control activities are designed to ensure that a high quality investigation and report have been provided. The following management tools can be used by investigative agencies to ensure quality investigations, and other techniques may be appropriate:

a. Case Review.

Case review consists of a supervisory review of the investigative requirements and the investigation to ensure that all coverage has been met using the best available sources. Depending on the agency, the investigative review may be conducted by the investigator's supervisor or by a quality assurance or assessment team.

b. Ride-Along Program.

In ride-along programs, supervisors and/or senior agents accompany the investigator, observing the investigator's performance, focusing on whether the investigator:

(1) Uses proper/acceptable investigative techniques.

(2) Explores all relevant issues.

(3) Possesses a demeanor that reflects positively on the investigative agency.

c. Source Recontact.

The supervisory element may select from a sample of an investigator's cases and contact some or all of the sources. The source is queried regarding the investigator's professionalism, line of questioning, adherence to established policies and procedures, and thoroughness. Both written and telephonic re-contact are acceptable.

These recommended monitoring activities ensure adequate training of investigators, acceptable supervisory oversight, and proper professionalism while conducting the investigation. They also ensure

that the standards of investigative coverage are satisfactorily met.

ANNEX C - Adjudication Guidelines for Determining Eligibility for Access to Classified Information.

This annex is identical to the presidentially-approved guidelines in the main topic titled Adjudicative Guidelines.

ANNEX D: Appeals Procedures -- Denial or Revocation of Access

1. Policy.

This annex establishes common appeals procedures for the denial or revocation of access to sensitive compartmented information (SCI) by entities of the Intelligence Community after adjudication pursuant to the provisions of DCID 6/4. This annex is promulgated pursuant to Executive Order 12333, Executive Order 12968, and the National Security Act of 1947, as amended. For the purposes of this annex, all references to DCID 6/4 include the basic document and all of its annexes. Any individual who has been considered for initial or continued access to SCI pursuant to the provisions of DCID 6/4 shall, to the extent provided below, be afforded an opportunity to appeal the denial or revocation of such access. This annex supersedes any and all other practices and procedures for the appeal of the denial or revocation of SCI access. This annex will not be construed to require the disclosure of classified information or information concerning intelligence sources and methods, nor will it be construed to afford an opportunity to appeal before the actual denial or revocation of SCI access. In addition, the provisions of DCID 6/4, or any other document or provision of law, will not be construed to create a liberty or property interest of any kind in the access of any individual to SCI.

2. Applicability.

This annex applies to all US Government civilian and military personnel, as well as any other individuals, including contractors and employees of contractors, who are considered for initial or continued access to SCI. This annex does not apply to decisions regarding employment and will not be construed to affect or impair public Law 88-290 or the authority of any entity to effect applicant or personnel actions pursuant to Public Law 88-290, Public Law 86-36, or other applicable law.

3. SCI Access Determination Authority.

Adjudications for access to SCI will be made in accordance with DCID 6/4 by a Determination Authority designated by the Senior Official of the Intelligence Community (SOIC) of each entity. Access to SCI shall be denied or revoked whenever it is determined that a person does not meet the security standards provided for in DCID 6/4. Any doubt about an individual's eligibility for access or continued access to SCI shall be resolved in favor of the national security and access will be denied or revoked.

4. Procedures.

a. Individuals will be:

(1) Provided as comprehensive and detailed a written explanation of the basis for that determination as the national security interests of the United States and other applicable law permit.

(2) Informed in this written explanation of their right to be represented by counsel or other representative at their own expense; to request any documents, records or reports upon which a denial or revocation is based; and, to request the entire investigative file as permitted by the national security and other applicable law.

(3) Provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy

Act (5 U.S.C. 552a), as applicable, any documents, records and reports upon which a denial or revocation is based.

(4) Provided an opportunity to reply in writing within 45 days of receipt of relevant documentation to request a review of the determination.

(5) Provided written notice of and reasons for the results of the review, the identity of the deciding authority in accordance with operational requirements, and written notice of the right to appeal.

(6) Provided an opportunity to appeal in writing to a high level panel, appointed by the SOIC, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final, except when the SOIC chooses to exercise the appeal authority personally, based on a recommendation from the panel, and provided to the individual.

(7) Provided an opportunity to appear personally and to present relevant documents, materials and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the SOIC. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection a.(6) of this section, in which case the written decision of the panel shall be made part of the applicant's or employee's security record.

b. When a SOIC or their principal deputy personally certifies that a procedure set forth in this section cannot be made available in a particular case without damaging the national security interests of the United States by revealing classified information, the particular procedure shall not be made available. This certification shall be conclusive.

c. Nothing in this annex shall prohibit a SOIC from personally exercising the appeal authority in paragraph a.(6) above based upon recommendations from an appeals panel. In such case, the decision of the SOIC shall be final.

d. A SOIC may determine that the appeal procedures prescribed in this annex cannot be invoked in a manner that is consistent with the national security. In such cases, a SOIC may deny an individual an appeal pursuant to this annex and the authority delegated to the SOIC by the DCI under the National Security Act of 1947, as amended. The SOIC's determination in this regard shall be conclusive.

e. The DCI or DDCI may take any actions regarding an individual's SCI access without regard to any of the provisions of this or any other regulation or directive. The DCI or DDCI may consult with the agency head pertaining to any action to be taken regarding an individual's SCI access.

f. This annex does not create nor confer on any person or entity any right to administrative or judicial review of these procedures, their implementation, or decisions or actions rendered thereunder. It also does not create or confer any right, benefit, or privilege, whether substantive or procedural, for access to classified information. Finally, this annex does not create or confer any substantive or procedural right, benefit, or privilege enforceable by any party against the United States or any agency, department, or instrumentality of the executive branch, its officers or employees, for any other person.

ANNEX E: Standards for SCI Security Awareness Programs in the US Intelligence Community

Consistent with controls and procedures set forth in DCID 1/19, "Security Policy for Sensitive Compartmented Information," and its supplement, "DCID 1/19 Security Policy Manual," standards are hereby established for the SCI security education programs designed to enhance the security awareness of the US Government civilian and military personnel and private contractors working in the US Intelligence Community. Compliance with these standards is required for all departments/agencies within the Intelligence Community. Existing security awareness programs will be modified to conform with these standards. Departments/agencies will establish a documented program to ensure that training has been presented to all personnel.

All individuals nominated for or holding SCI access approval will be notified initially and annually thereafter of their responsibility to report to their cognizant security officers any activities or conduct such as described in Annex C that could conflict with their ability to protect classified information from unauthorized disclosure. Any outside employment, activities or conduct that could create real or apparent conflicts with their responsibility to protect classified information must be reported.

The security awareness requirements set forth herein are divided into three phases. Phase 1 concerns the initial indoctrination of individuals, which is normally administered before access to SCI. Phase 2 concerns the continuing security awareness program required to maintain an increased security awareness throughout the period of access. Phase 3 sets forth the final guidelines and instructions when access to SCI is terminated.

1. Initial Indoctrination.

As soon as practicable after being approved for access to SCI, personnel will receive an initial security indoctrination that will include:

a. The need for and purpose of SCI, and the adverse effect on the national security that could result from unauthorized disclosure.

b. The intelligence mission of the department/agency to include the reasons why intelligence information is sensitive.

c. The administrative, personnel, physical, and other procedural security requirements of the department/agency and those requirements peculiar to specific duty assignments, including information on who to consult to determine if particular outside employment or activity might be of concern.

d. Individual classification management responsibilities as set forth in appropriate directives and regulations to include classification/declassification guidelines and marking requirements.

e. The definitions and criminal penalties for espionage, including harboring or concealing persons; gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information (Title 18, U.S.C., Sections 792 through 795, 797, and 798), the Internal Security

Act of 1950 (Title 50, U.S.C., Section 783), the Intelligence Identities Protection Act of 1982 (Title 50, U.S.C., Sections 421 through 426) and, when appropriate, the Atomic Energy Act (Sections 224 through 227).

f. The administrative sanctions for violation or disregard for security procedures.

g. A review of the techniques employed by foreign intelligence organizations in attempting to obtain national security information.

h. Individual security responsibilities including:

(1) The prohibition against discussing SCI in a non-secure area, over a non-secure telephone, or in any other manner that permits access by unauthorized persons.

(2) The need to determine, before disseminating SCI, that the prospective recipient has the proper security access approval, that the SCI is needed in order to perform official duties, and that the recipient can properly protect the information.

(3) The need to exercise security in activities as members of professional, commercial, scholarly or advocacy organizations that publish or discuss information on intelligence, defense or foreign affairs.

(4) The continuing obligation to submit for review any planned articles, books, speeches or public statements that contain or purport to contain SCI or information relating to or derived from SCI, as specified by the nondisclosure agreements that are a prerequisite for access to SCI.

(5) Obligation to report travel to or connections with countries with aggressive proactive intelligence capabilities, or contacts with foreign nationals under certain circumstances, or attempts (including blackmail, coercion and harassment) by unauthorized persons to obtain national security information, physical security deficiencies, and loss or possible compromise of SCI material.

(6) Obligation to report to proper authorities all activities or conduct of an individual who has access to SCI which relates to guidelines described in Annex C, such as:

(a) Involvement in activities or sympathetic association with persons which/who unlawfully practice or advocate the overthrow or alteration of the United States Government by unconstitutional means.
(b) Foreign influence concerns/close personal association with foreign nationals.
(c) Foreign citizenship or foreign monetary interests.
(d) Sexual behavior that is criminal or reflects a lack of judgment or discretion.
(e) Unwillingness to comply with rules and regulations or to cooperate with security processing.
(f) Unexplained affluence or excessive indebtedness.
(g) Alcohol abuse.
(h) Illegal or improper drug use/involvement.
(i) Apparent mental or emotional disorder(s).

(j) Criminal conduct.
(k) Noncompliance with security requirements.
(l) Engagement in outside activities which could cause a conflict of interest.
(m) Misuse of information technology systems.

(7) Identification of the elements in the department/agency to which matters of security interest are to be referred.

2. Periodic Awareness Enhancement.

Each department/agency will establish a continuing security awareness program that will provide frequent exposure of personnel to security awareness material. Implementation of a continuing program may include live briefings, audiovisual presentations (e.g., video tapes, films, and slide/tape programs), printed material (e.g., posters, memorandums, pamphlets, fliers), or a combination thereof. It is essential that current information and materials be utilized. Programs should be designed to meet the particular needs of the department/agency.

a. The basic elements for this program will include, but are not limited to, the following:

(1) The foreign intelligence threat (including the threats associated with foreign travel and foreign associations).

(2) The technical threat.

(3) Administrative, personnel, physical, and procedural security.

(4) Individual classification management responsibility.

(5) Criminal penalties and administrative sanctions.

(6) Individual security responsibilities.

(7) A review of other appropriate department/agency requirements.

b. Special security briefings/debriefings should supplement the existing security awareness programs in the following situations:

(1) When an individual is designated as a courier.

(2) When high risk situations are present, specifically:

(a) When an individual travels, officially or unofficially, to or through countries with aggressive/proactive intelligence capabilities or with connection(s) to terrorism or criminal activity, or:

(b) When an individual has, or anticipates contact with a representative(s) of the countries identified above.

(3) When any other situation arises for which the SOIC or designee determines that an increased level of protection is necessary.

3. Debriefing.

When a department/agency has determined that access to SCI is no longer required, final instructions and guidelines will be provided to the individual. At a minimum these shall include:

a. A requirement that the individual read appropriate sections of Titles 18 and 50, U.S.C., and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

b. The continuing obligation, under the prepublication and other provisions of the nondisclosure agreement for SCI, never to divulge; publish; or reveal by writing, word, conduct, or otherwise, to any unauthorized persons any SCI, without the written consent of appropriate department/agency officials.

c. An acknowledgment that the individual will report without delay to the Federal Bureau of Investigation, or the department/agency, any attempt by an unauthorized person to solicit national security information.

d. A declaration that the individual no longer possesses any documents or material containing SCI.

e. A reminder of the risks associated with foreign travel and foreign association.

ANNEX F: Reciprocity of SCI Eligibility Determinations

Annex F was signed by the DCI on 13 Oct 99.

1. Reciprocity Policy

a. Within the Intelligence Community, subject to the conditions set forth below, a favorable DCID 6/4 eligibility determination for access to SCI made by one adjudicative authority under SOIC cognizance is a favorable determination for all SOICS. Reciprocity of eligibility determinations does not in itself constitute reciprocity of need-to-know determinations. Need-to-know determinations are always distinct and separate decisions.

b. Reciprocity requires adjudication by trained government adjudicators under SOIC cognizance and a system for monitoring continuing security eligibility. Eligibility decisions, including the presence of exceptions, must be a matter of record accessible to the Intelligence Community's access granting authorities.

c. DCID 6/4 eligibility determinations are mutually acceptable and will not be readjudicated if:

(1) They are made without exception, and

(2) No substantial issue information exists since the most recent adjudication, and

(3) The appropriate type of polygraph examination, if one is required, has been satisfactorily completed.

d. Agencies may accept or reject DCID 6/4 eligibility determinations where exceptions exist based upon their own assessment of risk. Any agency rejecting another's determination of eligibility where exceptions exist will notify, to the extent it is able to do so, all adjudicative authorities having an eligibility interest in the person of its decision. Those authorities, in turn, may reassess the appropriateness of continuing to hold the person eligible with an exception.

e. Where an agency or organization has additional but not duplicative requirements, the actual granting of access is contingent upon satisfying those requirements. Failure to meet an additional but not duplicative requirement may not necessarily adversely affect a person's continued eligibility for reciprocal access with other organizations and agencies. However, the agency that made the original eligibility determination may use new information obtained by another organization to readjudicate the person's continued eligibility subject to restrictions placed on use of the information by the organization that obtained it.

f. A person determined ineligible for SCI access will remain ineligible for a minimum of one year. However, SOICs or their designees may waive this requirement in individual cases based on operational necessity and an assessment by the relevant determination authority that there is no unacceptable security risk in doing so.

g. This annex does not apply to suitability decisions for employment.

2. Definitions

a. Exception: An adjudicative decision to grant or continue access eligibility despite a failure to meet

adjudicative or investigative standards. Regarding SCI access eligibility, only the DCI or, as appropriate, the concerned Senior Official of the Intelligence Community (SOIC) or designee will make such decisions. An exception precludes reciprocity without review of the case by the gaining organization or program. There are three types:

(1) *Condition:* Access eligibility granted or continued with the proviso that one or more additional measures will be required. Such measures include additional security monitoring, restrictions on access, and restrictions on the individual's handling of classified information. Submission of periodic financial statements, admonishment regarding use of drugs or excessive use of alcohol, and satisfactory progress in a government-approved counseling program are examples of conditions.

(2) *Deviation:* Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or an out-of-date investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of six months or more within the most recent five years investigated or the lack of an FBI name check or technical check or the lack of one or more relevant investigative scope components (e.g., employment checks or a subject interview for an SSBI, financial review for any investigation) in its entirety.

(3) *Waiver:* Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access. The DCI, SOIC, or SOIC's designee approve waivers pursuant to their authorities outlined in DCID 6/4, paragraphs 6a and b, only when the benefit of access clearly outweighs any security concern raised by the shortcoming. A waiver may require special limitations on access, additional security monitoring and other restrictions on the person's handling of classified information beyond normal need-to-know. Paragraph 6 of DCID 6/4 governs the granting of waivers insofar as they pertain to SCI access eligibility. In the Intelligence Community, waivers may be contemplated when the person under consideration for SCI access is not a United States citizen, when any member of that person's immediate family is not a US citizen, or when any member of the immediate family or other person with whom there is a bond of affection or obligation is subject to duress.

b. *Issue information:* Any information that could adversely affect a person's eligibility for access to classified information. There are two types:

(1) *Minor issue information:* Information that meets a threshold of concern set out in "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" (see Annex C to DCID 6/4), but for which adjudication determines that adequate mitigation, as provided for by the Guidelines, exists. Minor issue information does not provide the basis for a waiver or condition.

(2) *Substantial issue information:* Any information, or aggregate of information, that raises a significant question about the prudence of granting access eligibility. Substantial issue information constitutes the basis for granting access eligibility with waiver or condition, or for denying or revoking access eligibility. Granting access eligibility when substantial issue information exists is predicated upon meeting the requirements of paragraphs 12a and b of DCID 6/4 for tailored security programs whose purpose is to resolve issues.

c. *Need to know:* A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

d. *Reciprocity:* Acceptance by one SOIC of an SCI access eligibility determination made by another. It applies both to granting access when another SOIC has approved and denying access when another SOIC has denied or revoked. Reciprocity does not include agency determinations of employment suitability. Nothing precludes SOICs or their designees from exercising authority to grant or to deny access for reasons of operational necessity regardless of another SOIC's decision.

3. The Effect of the Polygraph on Reciprocity

The Intelligence Community uses the polygraph in defined circumstances to provide additional information to the adjudicative process. Reciprocity of an SCI eligibility determination when a polygraph requirement exists is conditional upon satisfactory completion of that requirement.

4. Review of Access Determinations

All denials or revocations of access eligibility are subject to the review proceedings outlined in Annex D, above.

Adjudicative Guidelines For Determining Eligibility for Access To Classified Information

Approved by the President March 24, 1997

A. Introduction

The following adjudicative guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information (SCI) and special access programs (SAPs) and are to be used by government departments and agencies in all final clearance determinations.

B. Adjudicative Process

1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

a. The nature, extent, and seriousness of the conduct;
b. The circumstances surrounding the conduct, to include knowledgeable participation;
c. The frequency and recency of the conduct;
d. The individual's age and maturity at the time of the conduct;
e. The voluntariness of participation;
f. The presence or absence of rehabilitation and other pertinent behavioral changes;
g. The motivation for the conduct;
h. The potential for pressure, coercion, exploitation, or duress; and

i. The likelihood of continuation or recurrence.

2. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

a. Guideline A: Allegiance to the United States
b. Guideline B: Foreign influence
c. Guideline C: Foreign preference
d. Guideline D: Sexual behavior
e. Guideline E: Personal conduct
f. Guideline F: Financial considerations
g. Guideline G: Alcohol consumption
h. Guideline H: Drug involvement
i. Guideline I: Emotional, mental, and personality disorders
j. Guideline J: Criminal conduct
k. Guideline K: Security violations
l. Guideline L: Outside activities
m. Guideline M: Misuse of information technology systems

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

5. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

a. Voluntarily reported the information;
b. Was truthful and complete in responding to questions;
c. Sought assistance and followed professional guidance, where appropriate;
d. Resolved or appears likely to favorably resolve the security concern;
e. Has demonstrated positive changes in behavior and

employment;
f. Should have his or her access temporarily suspended pending final adjudication of the information.

6. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

Guideline A
Allegiance to the United States

The Concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

c. Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means;

d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

c. Involvement in the above activities occurred for only a short

period of time and was attributable to curiosity or academic interest;

d. The person has had no recent involvement or association with such activities.

Guideline B
Foreign Influence

The Concern. A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and may be disqualifying include:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

c. Relatives, cohabitants, or associates who are connected with any foreign government;

d. Failing to report, where required, associations with foreign nationals;

e, Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

f. Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual

vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

a. A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

b. Contacts with foreign citizens are the result of official U.S. Government business;

c. Contact and correspondence with foreign citizens are casual and infrequent;

d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

Guideline C
Foreign Preference

The Concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. The exercise of dual citizenship;

b. Possession and/or use of a foreign passport;

c. Military service or a willingness to bear arms for a foreign country;

d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

f. Residence in a foreign country to meet citizenship requirements;

g. Using foreign citizenship to protect financial or business interests in another country;

h. Seeking or holding political office in the foreign country;

h. Voting in foreign elections; and

i. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

c. Activity is sanctioned by the United States;

d. Individual has expressed a willingness to renounce dual citizenship.

Guideline D
Sexual Behavior

The Concern. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. (see footnote) Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Conditions that could raise a security concern and may be disqualifying include:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or which is symptomatic of a personality disorder;

c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation or duress;

d. Sexual behavior of a public nature and/or which reflects lack

of discretion or judgment.

Conditions that could mitigate security concerns include:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

Footnote: The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J); or emotional, mental, and personality disorders (Guideline I), in determining how to resolve the security concerns raised by sexual behavior.

Guideline E
Personal Conduct

The Concern. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

b. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security

questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

d. Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

e. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency.

f. Association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;

g. Association with persons involved in criminal activities has ceased.

Guideline F
Financial Considerations

The Concern. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying include:

a. A history of not meeting financial obligations;

b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

c. Inability or unwillingness to satisfy debts;

d. Unexplained affluence;

e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

a. The behavior was not recent;

b. It was an isolated incident;

c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

e. The affluence resulted from a legal source; and

f. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

Guideline G
Alcohol Consumption

The Concern. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and may be disqualifying include:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

e. Habitual or binge consumption of alcohol to the point of impaired judgment;

f. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program

Conditions that could mitigate security concerns include:

a. The alcohol related incidents do not indicate a pattern;

b. The problem occurred a number of years ago and there is no indication of a recent problem;

c. Positive changes in behavior supportive of sobriety;

d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed

clinical social worker who is a staff member of a recognized alcohol treatment program.

Guideline H
Drug Involvement

The Concern.

a. Improper or illegal involvement with drugs, raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

b. Drugs are defined as mood and behavior altering substances and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and
(2) Inhalants and other similar substances.

c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualifying include:

a. Any drug abuse (see above definition);

b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

e. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

Conditions that could mitigate security concerns include:

a. The drug involvement was not recent;

b. The drug involvement was an isolated or aberrational event;

c. A demonstrated intent not to abuse any drugs in the future;

d. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

Guideline I
Emotional, Mental, and Personality Disorders

The Concern. Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to, or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

Conditions that could raise a security concern and may be disqualifying include:

a. An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g. failure to take prescribed medication;

c. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Conditions that could mitigate security concerns include:

a. There is no indication of a current problem;

b. Recent opinion by a credentialed mental health professional

that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission and has a low probability of recurrence or exacerbation;

c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

Guideline J
Criminal Conduct

The Concern. A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

a. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

b. A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

a. The criminal behavior was not recent;

b. The crime was an isolated incident;

c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;

e. Acquittal

f. There is clear evidence of successful rehabilitation.

Guideline K
Security Violations

The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

a. Unauthorized disclosure of classified information;

b. Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

a. Were inadvertent;

b. Were isolated or infrequent;

c. Were due to improper or inadequate training;

d. Demonstrate a positive attitude towards the discharge of security responsibilities.

Guideline L
Outside Activities

The Concern. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include:

Any service, whether compensated, volunteer, or employment with:

a. A foreign country;

b. Any foreign national;

c. A representative of any foreign interest;

d. Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

b. The individual terminates the employment or discontinues

the activity upon being notified that it is in conflict with his or her security responsibilities.

Guideline L
Misuse of Information Technology Systems

The Concern. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

a. Illegal or unauthorized entry into any information technology system;

b. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;

c. Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

d. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

Conditions that could mitigate security concerns include:

a. The misuse was not recent or significant;

b. The conduct was unintentional or inadvertent;

c. The introduction or removal of media was authorized;

d. The misuse was an isolated event;

e. The misuse was followed immediately by a prompt, good faith effort to correct the situation.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND CONTROL. COMMUNICATIONS, AND INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENT
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Personnel Security Investigations and Adjudications

On March 24, 1997, the President approved the uniform Adjudicative Guidelines (Attachment 1), and Temporary Eligibility Standards and Investigative Standards (Attachment 2) required by Executive Order 12968, "Access to Classified Information." These guidelines and investigative standards supersede that contained in Change 3 to DoD 5200.2-R, -DoD Personnel Security Program," dated February 23, 1996 and subsequent policy memoranda on the same subject.

Of particular note are the investigative standards for access to Secret and Confidential information, to include Special Access Program (SAP) information. The investigative and reinvestigative scope for Secret and Confidential access will consist of a National Agency Check, Local Agency Checks and Credit Check (NACLQ. Also, individuals with Secret access will be subject to a periodic reinvestigation (PR) every 10 years and for those with Confidential access, every 15 years. The cost of the new investigative standards for access to Secret and Confidential information are offset by the reduction in cost for the single scope background investigation and afford the Department enhanced security protection against the insider threat. The investigative standards for access to Top Secret and Sensitive Compartmented Information were implemented by the ASD(C31) on July 1, 1996.

Effective January 1, 1999, the Defense Security Service (DSS) will begin implementing the NACLC investigative and reinvestigative requirement for Secret and Confidential access. Implementation details are contained in Attachment 3. The E.O. 10450 investigative requirement for civilian employment remains unchanged. The National Agency Check with Written Inquiries and credit check (NACIC) or Access NACIC (ANACI) will continue to serve as the basis for Secret & Confidential clearances for civilian employees of the Department.

This policy will be incorporated into the next version of DoD 5200.2-R not later than January 1, 2000.

signed November 10, 1998

Arthur L. Money
Senior Civilian Official

Attachments

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY

FOR ACCESS TO CLASSIFIED INFORMATION

A. INTRODUCTION

The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information and/or assignment to sensitive national security positions. They apply to persons being considered for initial or continued eligibility for assignment to sensitive positions and/or access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs) and are to be used by government departments and agencies in all final clearance detertru nations.

B. ADJUDICATIVE PROCESS

1 . The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

a. The nature, extent, and seriousness of the conduct;

b. The circumstances surrounding the conduct, to include knowledgeable participation;

c. The frequency and recency of the conduct;

d. The individual's age and maturity at the time of the conduct;

e. The voluntariness of participation;

f. The presence or absence of rehabilitation and other pertinent behavioral changes;

g. The motivation for the conduct;

h, The potential for pressure, coercion, exploitation, or duress; and

i. The likelihood of continuation or recurrence.

2. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

a. Guideline A: Allegiance to the United States

b. Guideline B: Foreign influence

c. Guideline C: Foreign preference

d. Guideline D: Sexual behavior

e. Guideline E: Personal conduct

I. Guideline F: Financial considerations

g. Guideline G: Alcohol consumption

h. Guideline H: Drug involvement

i. Guideline I: Emotional, mental, and personality disorders

j. Guideline J: Criminal conduct

k. Guideline K: Security Violations

1. Guideline L: Outside activities

m. Guideline M: Misuse of Information Technology Systems

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may he disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

5. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

a. Voluntarily reported the information

b. Was truthful and complete in responding to questions

c. Sought assistance and followed professional guidance, where appropriate

d. Resolved or appears likely to favorably resolve the security concern

e. Has demonstrated positive changes in behavior and employment

f. Should have his or her access temporarily suspended pending final adjudication of the information.

6. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

GUIDELINE A

Allegiance to the United States

The Concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

c. Association or sympathy with persons or organizations that advocate the overthrow of the U.S. Government, or any state or subdivision, by force or violence or by other unconstitutional means;

d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

c. Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

d. The person has had no recent involvement or association with such activities-

GUIDELINE B

Foreign Influence

The Concern: A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom be or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and may be disqualifying include:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

c. Relatives, cohabitants, or associates who are connected with any foreign government;

d. Failing to report, where required, associations with foreign nationals;

e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

f. Conduct, which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

a. A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

b. Contacts with foreign citizens are the result of official United States Government business;

c. Contact and correspondence with foreign citizens are casual and infrequent;

d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

GUIDELINE C

Foreign Preference

The Concern: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. The exercise of dual citizenship;

b. Possession and/or use of a foreign passport;

c. Military service or a willingness to bear arms for a foreign country;

d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

e. Residence in a foreign country to meet citizenship requirements;

f. Using foreign citizenship to protect financial or business interests in another country.

g. Seeking or holding political office in the foreign country;

h. Voting in foreign elections; and

i. Performing or attempting to perform duties, or other-wise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

c. Activity is sanctioned by the United States;

d. Individual has expressed a willingness to renounce dual citizenship.

GUIDELINE D

Sexual Behavior

The Concern: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. [i] Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Conditions that could raise a security concern and may be disqualifying include:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

d. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

Conditions that could mitigate security concerns include:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

i The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline 1) in determining how to resolve the security concerns raised by sexual behavior.

GUIDELINE E

Personal Conduct

The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

b. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination,

d. Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

e. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency,

f. Association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements, and upon being made aware of the requirement, fully and truthfully provided the requested information;

g. Association with persons involved in criminal activities has ceased.

GUIDELINE F

Financial Considerations

The Concern: An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying include:

a. A history of not meeting financial obligations;

b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

c. Inability or unwillingness to satisfy debts;

d. Unexplained affluence;

e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

a. The behavior was not recent;

b. It was an isolated incident;

c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

e. The affluence resulted from a legal source; and

f. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

GUIDELINE G

Alcohol Consumption

The Concern: Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and may be disqualifying include:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

e. Habitual or binge consumption of alcohol to the point of impaired judgment;

L Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of a alcohol rehabilitation program.

Conditions that could min : gate security concerns include:

a. The alcohol-related incidents do not indicate a pattern;

b. The problem occurred a number of years ago and there is no indication of a recent problem-,

c. Positive changes in behavior supportive of sobriety;

d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participated frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H

Drug Involvement

The Concern:

a. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

b. Drugs are defined as mood and behavior-altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) Inhalants and other similar substances.

c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualiffing include:

a. Any drug abuse (see above definition);

b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution,

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

e. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

Conditions that could mitigate security concerns include:

a. The drug involvement was not recent;

b. The drug involvement was an isolated or aberrational event;

c. A demonstrated intent not to abuse any drugs in the future;

d. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

GUIDELINE I

Emotional, Mental, and Personality Disorders

The Concern: Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

Conditions that could raise a security concern and may be disqualifying include:

a. An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

c. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Conditions that could mitigate security concerns include:

a. There is no indication of a current problem-,

b. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission, and has a low probability of recurrence or exacerbation;

c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

GUIDELINE J

Criminal Conduct

The Concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

a. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

b. A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

a. The criminal behavior was not recent;

b. The crime was an isolated incident,

c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur-,

e. Acquittal;

f. There is clear evidence of successful rehabilitation.

GUIDELINE K

Security Violations

The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

a. Unauthorized disclosure of classified information;

b. Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

a. Were inadvertent;

b. Were isolated or infrequent;

c. Were due to improper or inadequate training;

d. Demonstrate a positive attitude towards the discharge of security responsibilities.

GUIDELINE L

Outside Activities

The Concern: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:

a. A foreign country;

b. Any foreign national;

c. A representative of any foreign interest;

d. Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

GUIDELINE M

Misuse of Information Technology Systems

The Concern: Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

a. Illegal or unauthorized entry into any information technology system;

b. Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

c. Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

d, Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Conditions that could mitigate security concerns include:

a, The misuse was not recent or significant;

b. The conduct was unintentional or inadvertent;

c. The introduction or removal of media was authorized;

d. The misuse was an isolated event;

e. The misuse was followed by a prompt, good faith effort to correct the situation.

INVESTIGATIVE STANDARDS FOR BACKGROUND INVESTIGATIONS

FOR

ACCESS TO CLASSIFIED INFORMATION'

A. INTRODUCTION

The following investigative standards have been established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs), and constitute the investigative basis for final clearance determinations. However, nothing in these standards prohibits the Department of Defense from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

B. THE THREE STANDARDS

There are three standards (Table I summarizes when to use each one):

1. The investigation and reinvestigation standard for access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by Section 4.4 of Executive Order 12958);

2. The investigation standard for access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

3. The reinvestigation standard for continued access to the levels listed in subsection B.2, above.

C. EXCEPTIONS TO PERIODS OF COVERAGE

Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the subject's 18th birthday to the present or to two years, whichever is longer.

Comment: However, no investigation shall be conducted prior to an individual's 16th birthday. Additionally, lack of coverage in any investigative category shall be compensated for through other investigative means.

Italized type is used to amplify the standards in certain areas for implementation within DoD.

D. **EXPANDING INVESTIGATIONS**

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

E. **TRANSFERABILITY**

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

F. **BREAKS IN SERVICE**

If a person who requires access has been retired or separated from U.S. Government employment for less than 24 months and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated SF 86 *(or EPSQ)* and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of this Regulation.

G. **THE NATIONAL AGENCY CHECK (NAQ)** The NAC is a part of all investigations and reinvestigations.

Comment: The scope for the NAC is five years or to age 18, whichever is the shorter period.

At a minimum, it consists of a review of the following-

1. Investigative and criminal history files of the FBI, including a technical fingerprint search;

a. FB11HQ has on file copies of investigations conducted by the FBI. TheFB11HQ check consists of a review of files for information of a security nature and that developed during applicant-type investigations.

b. FBI17D check (excluding EATNACs) is based upon a technical fingerprint search that consists of a classification of the subject's fingerprints and a comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a "name check only" of these files is automatically conducted.

2. OPM's Security/Suitability Investigations Index (SU): *The files of OPM contain the results of investigations conducted by OPM under Executive Order 10450, those requested by the NRC, the DOE, and those requested since August 1952 to serve as a basis for "Q" clearances.*

Additionally, personnel security adjudicative determinations rendered by other federal agencies are contained in the SII. OPM S11 records will be checked on all subjects of DoD investigations.

3. Defense Clearance and Investigations Index (DCH): *The DCII data base consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained b - v DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained by subject in the DCII. DCII re cords will be checked on all subjects of DoD investigations.*

4. Such other national agencies (e.g., CIA, INS) appropriate to the individual's background.

a. *Central Intelligence Agency (CIA . The CIA maintains the following records:*

(1) Directorate of Operations (CIA-DO/1MS) maintains the Foreign Intelligence Counterintelligence database. This database shall be checked for all foreign nationals residing outside the U.S. requiring access to classified infor7nation (i.e., LAA). If the requester provides complete personal identifying information (complete name, date of birth, place of birth, and citizenship), all alien co-subjects (on SSBIs) residing outside the U.S. are also checked In addition, this database shall be queried on the subject any time there is a counterintelligence concern raised during the conduct of the PSI.

(2) Office of Security (CJA-OS) maintains information on present and former employees, including members of the Office of Strategic Services (OSS), and applicants for employment. These files shall be checked if subject has been an employee of the CIA or when other sources indicate that the CIA may have pertinent information.

b. Immigration and Naturalization Service (I&NS :The files of I&NS contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declarations of intention, visitor's visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the United States. I&NS records are checked when the subject is:

(])An alien in the U.S., or

(2) A naturalized citizen whose naturalization has not been verified, or

(3) An immigrant alien, or

***(4) A U.S. citizen who received derivative citizenship through the naturalization** of one or both parents provided that such citizenship has not been verified in a prior investigation.*

c. State Department :The State Department maintains the following records:

(1) Security Division files contains information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

(2) Passport Division files shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where helshe was born. Verification of this registration is verification of citizenship.

d. Military Personnel Record Center: Files are maintained by separate departments of the Armed Forces, General Services Administration, and the Reserve Records Centers. They consist of the master personnel records of retired, separated, reserve, and active duty members of the Armed Forces.

***Comment:** Military requesters must review service records of any active duty member at the time the investigation is requested. Unfavorable information must be recorded on the investigative request form. Review ofprior military service records is to be conducted by the investigating agency through the Defense Manpower Data Center databases or the Military Personnel Record Center files, as appropriate.*

e. Treasury Department: The files of Treasury Department agencies (Secret Service, Internal Revenue Service, and Bureau of Customs) shall be checked only when available information indicates that an agency of the Treasury Department may be reasonably expected to have pertinent information.

f *7hefiles of other agencies such as the National Guard Bureau, etc. shall be checked when pertinent to the purpose for which the investigation is being conducted.*

H. NATIONAL AGENCY CHECK WITH LOCAL AGENCY CHECKS AND CREDIT CHECK(NACLC)

1. Applicability: The NACLC applies to the investigations and reinvestigations conducted to determine eligibility for access to CONFIDENTIAL and SECRET (including all SECRET level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section 4.4, E.O. 12958).

2. For Reinvestigations: When to Reinvestigate. The reinvestigation may be initiated at any time following completion of, but not later than ten years for SECRET (15 years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation including when there has been a break in service.).

3. Investigative Requirements:

a. Completion of Forms. Completion of SF 86 *(or EPSQ)* including applicable releases and supporting documentation;

b. National Agency Check. Completion of a NAC.

Comment: For Secret and Confidential periodic reinvestigations, fingerprint cards are not required if there is a previous valid technical check of the FBI.

c. Financial Review: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

d. Date and Place of Birth: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation, and a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

Comment: Verification of date and place of birth by sighting an original or certified copy of a birth certificate or other acceptable documentation should nor7nally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance.

e. Local Agency Checks: As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last five years, and, if applicable, of the appropriate agency for any identified arrests.

f. Expanding the Investigation. The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

1. SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)

1. Applicability : The initial investigation for access to TOP SECRET (including TOP SECRET SAPs), SCI, and occupancy of a critical sensitive position.

2. Investigative Requirements:

a. Completion of Forms. Completion of SF 86 *(or EPSQ),* as appropriate, including applicable releases and supporting documentation;

b. National Agency Check. Completion of a NAC.

c. National Agency Check for the Spouse or Cohabitant (if applicable - Completion of a NAC, without fingerprint cards, for the spouse or cohabitant.

d. Date and Place of Birth. Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

Comment: Verification of date and place of birth by sighting an original or certified copy of a birth certificate or other acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the DD 1879 should be annotated to this effect.,

e. Citizenship. For individuals born outside the United States, verification of U.S. citizenship directly from the appropriate registration authority; verification of U.S. citizenship or legal status of foreign-born immediate fan-Lily members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

Comment: Verification of citizenship by sighting of acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the DD 1879 should be annotated to this effect. For individuals born outside the U.S., the investigating agency will verify citizenship directl yfrom the appropriate registration authority and also, verify U.S. citizenship or legal status of foreign-born immediate family members.

Acceptable proofs of citizenship are as follows:

(1) For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office. The only exception is a state or other jurisdiction that does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable.

(2) A delayed birth certificate is one created when a record was filed more than one year after the date of birth. Such a certificate is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include: baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of birth. Other documentary evidence can be early census, school, or family bible records, newspaper files, or insurance papers.

(3) All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

(4) If the individual claims citizenship by naturalization, a certificate of naturalization shall be submitted.

(5) If citizenship was acquired by birth abroad to a U. S. citizen parent or parents, the following are acceptable evidence:

(a) A Certificate of Citizenship issued by the Immigration and Naturalization Service (I&NS); or

(b) A Report of Birth Abroad of *a Citizen of the United States* of *America (Form FS-240); or*

(c) A Certificate of *Birth (For7n FS-545 or DS-1350).*

(d) A passport or one in which the individual was included will be accepted as proof of citizenship.

f. Education. Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education was a primary activity of the subject during the most recent three years.

Comment: Corroboration of education within the scope of investigation shall normally be accomplished by the requester prior to the initiation of the request for investigation. If all education is outside of the investigative scope, the last education above high school level will be verified.

9. Employment. Verification of all employments for the past seven years; personal interviews of sources (supervisors, coworkers, Or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding 60 days; verification of all prior federal and military service, including type of discharge. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments. However, each duty location must be individually listed.

Comment: *For Federal employees, all service within one agency of the Federal Government will be considered as one employment, regardless 9f assignment. However, each duty location must be individually listed.*

h. References. Four references, of whom at least two are developed; to the extent praeticable, all should have social knowledge of the subject and collectively span at least the last seven years.

i. Former Spouse. An interview of any former spouse divorced within the last ten years.

j. Neighborhoods, Confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

Comment: The SSBI standard for neighborhoods allows an investigative entity sufficient flexibility to meet the standard, provided that a reasonable effort is made to obtain coverage within the investigative period and the lack of coverage in any investigative category should be compensated for through other investigative means.

k. Financial Review. Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

1. Local Agency Checks. A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and /or attended school for six months or more, including current residence regardless of duration. If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.

m. Public Records. Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.

n. Subject Interview. A subject inter-view, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

o. Polygraph (only in agencies with approved personnel security polygraph programs). In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

3. Expanding the Investigation. The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

J. SINGLE SCOPE BACKGROUND INVESTIGATION - PERIODIC REINVESTIGATION (SSBI-PR)

1. Applicability . Applies to reinvestigations for access to TOP SECRET (including TOP SECRET SAPs), SCI.

Comment: Also, applies to eligibility for occupancy of a critical sensitive position.

2. When to Reinvestigate. The reinvestigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation (see Table 2).

Comment: The investigation will cover the most recent five year period or the period since the last investigation, whichever is shorter.

3. Reinvestigate Requirements. Reinvestigate requirements are as follows:

a. Completion of Forms. Completion of SF 86 *(or EPSQ)*, as appropriate, including applicable releases and supporting documentation.

b. National Agency Check. Completion of a NAC (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).

c. National Agency Check for the Spouse or Cohabitant (if applicable). Completion of a NAC, without fingerprint cards, for the spouse or cohabitant. The NAC for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.

d. Employment. Verification of 0 employments since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employment of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

Comment: For Federal employees, all service within one agency of the Federal Government will be considered as one employment, regardless of assignment.

e. References. Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practicable, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

f. Neighborhoods. Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

Comment: The SSBI-PR standard for neighborhoods allows any investigative entity sufficient flexibility to meet the standard, providing that a reasonable effort is made to obtain coverage within the investigative period and that lack of coverage in any investigative category should be compensated for through other investigative means.

g. Financial Review.

1) Financial Status. Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) Check of Treasury's Financial Database. Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign banks and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

h. Local Agency Checks. A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.

i. Former Spouse. An inter-view with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.

Comment: An interview will be conducted with any former spouse whose divorce from Subject took place after the date of the last investigation or reinvestigation (regardless of how long the interval).

j. Public Records. Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

k. Subject Interview. A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject inter-views may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

4. Expanding the Reinvestigation. The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

K. INVESTIGATIVE STANDARDS FOR TENTORARY ELIGIBILITY FOR ACCESS

1. Introduction. Minimum investigative standards, implementing Section 3.3 of Executive Order 12968, are established for all DoD military personnel, civilian employees, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other personnel who require access to classified information before the appropriate investigation can be completed and a final determination made,

2. Temporary Eligibility for Access . In exceptional circumstances where official functions must be performed prior to completion of the investigation and adjudication process, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

a. CONFIDENTIAL and SECRET Levels. As a minimum, such temporary eligibility requires completion of the SF 86 (or *EPSQ)*, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, a DCII check, and submission of an expedited request for an NACLC.

b. TOP SECRET and SCI Levels For someone who is the Subject of a Favorable Investigation Not Meeting the Investigative Standards for Access at Those Levels. As a minimum, such temporary eligibility requires completion of the SF 86 (or *EPSQ)*, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for an SSBL

c. TOP SECRET and SCI Levels For someone who is Not the Subject of a Current, Favorable Personnel or Personnel-Security Investigation of Any Kind. As a minimum, such temporary eligibility requires completion of the SF 86 (or *EPSQ)*, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited SSBI, and completion and favorable review by the appropriate adjudicating authority of relevant crirninal history and investigative records of the FBI and of information in the Security/Suitability Investigations Index (SIT) and the DCIL

d. Additional Requirements by Agencies. Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified in formation necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations as contained in this Regulation. Temporary eligibility for access is valid only at the agency granting it and at other agencies that expressly agree to accept it and acknowledge understanding of its investigative basis. Where temporary eligibility for access is granted under the provisions of this section, or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the subject access to its information.

DECISION TABLES

TABLE 1: WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investiation required is	Using standard
CONFIDENTIAL SECRET	none	none	NACLC	H
	CONFIDENTIAL SECRET; "L"	out of date NAC, ENTNAC, NACIC, NACLC, BI, SBI, or SSBI		
TOPSECRET, SCI:	none	none	SSBI	I
	none; CONF, SEC; "L"	current or out of date NAC, ENTNAC, NACIC, NACLC, BI, SBI		
	TS, SCI; "Q"	out of date SSBI	SSBTPR	I

TABLE 2: REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service or employment of		*Type required if there has been a break in access (no access1lower level* of *access) but remains in military service, federal service, or with same employer in industry*
		0-23 mos.	24 mos. or more	
CONFIDENTIAL	0 to 14 yrs. 11 mos.	None	NACLC	*None*
	15 yrs. or more	NACLC-PR	NACLC	*NACLC-PR*
SECRET	0 to 9 yrs. 11 mos.	None	NACLC	*None*
	1 O yrs. or more	NACUC-PR	NACLC	*NACLC-PR*
TOP SECRET, SCI	0 to 4 yrs. 11 mos,	None (Note 2)	SSBJ	*None*
	5 yrs. or more	SSBI-PR	SSBI	SSBI-PR

NOTE 1: The NACLC investigative and reinvestigate requirement for Secret and Confidential access will begin January 1, 1999. Personnel with an existing NACIENTNAC completed prior to January 1, 1999 and who have prior security clearance eligibility, will not require a NACLC to maintain their Secret or Confidential clearance. However, personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and no prior security

clearance eligibility, will require a NACLC for issuance of a Secret or Confidential clearance, regardless of the age of the investigation.

NOTE 2: As a minimum, review an updated SF-86 and applicable records. A reinvestigation SSBI-PR is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 1296&

Implementation of the NACLC

- Any National Agency Check (NAC) or Entrance NAC (ENTNAC) submitted for a Secret or Confidential clearance and opened by DSS prior to January 1, 1999, will be eligible for issuance of a security clearance.

- Any Secret/Confidential clearance request opened by DSS after January 1, 1999 will be run as a NACLC, this includes enlisted and officer accessions. Requests not indicating the investigation is for a clearance will continue to be run as a NAC or ENTNAC.

- Personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and who have a prior security clearance eligibility, will not require a NACLC to maintain their Secret or Confidential clearance. However, personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and no prior security clearance eligibility, will require a NACLC for issuance of a Secret or Confidential clearance, regardless of the age of the investigation.

- An NACIC and ANACI will serve as the basis for issuance of Secret or Confidential clearances for civilian employees.

Attachment 3

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND CONTROL. COMMUNICATIONS, AND INTELLIGENCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENT
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES

SUBJECT: Personnel Security Investigations and Adjudications

On March 24, 1997, the President approved the uniform Adjudicative Guidelines (Attachment 1), and Temporary Eligibility Standards and Investigative Standards (Attachment 2) required by Executive Order 12968, "Access to Classified Information." These guidelines and investigative standards supersede that contained in Change 3 to DoD 5200.2-R, -DoD Personnel Security Program," dated February 23, 1996 and subsequent policy memoranda on the same subject.

Of particular note are the investigative standards for access to Secret and Confidential information, to include Special Access Program (SAP) information. The investigative and reinvestigative scope for Secret and Confidential access will consist of a National Agency Check, Local Agency Checks and Credit Check (NACLQ. Also, individuals with Secret access will be subject to a periodic reinvestigation (PR) every 10 years and for those with Confidential access, every 15 years. The cost of the new investigative standards for access to Secret and Confidential information are offset by the reduction in cost for the single scope background investigation and afford the Department enhanced security protection against the insider threat. The investigative standards for access to Top Secret and Sensitive Compartmented Information were implemented by the ASD(C31) on July 1, 1996.

Effective January 1, 1999, the Defense Security Service (DSS) will begin implementing the NACLC investigative and reinvestigative requirement for Secret and Confidential access. Implementation details are contained in Attachment 3. The E.O. 10450 investigative requirement for civilian employment remains unchanged. The National Agency Check with Written Inquiries and credit check (NACIC) or Access NACIC (ANACI) will continue to serve as the basis for Secret & Confidential clearances for civilian employees of the Department.

This policy will be incorporated into the next version of DoD 5200.2-R not later than January 1, 2000.

signed November 10, 1998

Arthur L. Money
Senior Civilian Official

Attachments

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY

FOR ACCESS TO CLASSIFIED INFORMATION

A. INTRODUCTION

The following adjudicative guidelines are established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information and/or assignment to sensitive national security positions. They apply to persons being considered for initial or continued eligibility for assignment to sensitive positions and/or access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs) and are to be used by government departments and agencies in all final clearance detertru nations.

B. ADJUDICATIVE PROCESS

1 . The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

a. The nature, extent, and seriousness of the conduct;

b. The circumstances surrounding the conduct, to include knowledgeable participation;

c. The frequency and recency of the conduct;

d. The individual's age and maturity at the time of the conduct;

e. The voluntariness of participation;

f. The presence or absence of rehabilitation and other pertinent behavioral changes;

g. The motivation for the conduct;

h, The potential for pressure, coercion, exploitation, or duress; and

i. The likelihood of continuation or recurrence.

2. Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

a. Guideline A: Allegiance to the United States

b. Guideline B: Foreign influence

c. Guideline C: Foreign preference

d. Guideline D: Sexual behavior

e. Guideline E: Personal conduct

I. Guideline F: Financial considerations

g. Guideline G: Alcohol consumption

h. Guideline H: Drug involvement

i. Guideline I: Emotional, mental, and personality disorders

j. Guideline J: Criminal conduct

k. Guideline K: Security Violations

1. Guideline L: Outside activities

m. Guideline M: Misuse of Information Technology Systems

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may he disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

5. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

a. Voluntarily reported the information

b. Was truthful and complete in responding to questions

c. Sought assistance and followed professional guidance, where appropriate

d. Resolved or appears likely to favorably resolve the security concern

e. Has demonstrated positive changes in behavior and employment

f. Should have his or her access temporarily suspended pending final adjudication of the information.

6. If after evaluating information of security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend approval with a warning that future incidents of a similar nature may result in revocation of access.

GUIDELINE A

Allegiance to the United States

The Concern. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;

b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;

c. Association or sympathy with persons or organizations that advocate the overthrow of the U.S. Government, or any state or subdivision, by force or violence or by other unconstitutional means;

d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

Conditions that could mitigate security concerns include:

a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;

b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;

c. Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;

d. The person has had no recent involvement or association with such activities-

GUIDELINE B

Foreign Influence

The Concern: A security risk may exist when an individual's immediate family, including cohabitants and other persons to whom be or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Conditions that could raise a security concern and may be disqualifying include:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;

c. Relatives, cohabitants, or associates who are connected with any foreign government;

d. Failing to report, where required, associations with foreign nationals;

e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;

f. Conduct, which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;

g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;

h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

Conditions that could mitigate security concerns include:

a. A determination that the immediate family member(s) (spouse, father, mother, sons, daughters, brothers, sisters), cohabitant, or associate(s) in question are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force the individual to choose between loyalty to the person(s) involved and the United States;

b. Contacts with foreign citizens are the result of official United States Government business;

c. Contact and correspondence with foreign citizens are casual and infrequent;

d. The individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons or organizations from a foreign country;

e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

GUIDELINE C

Foreign Preference

The Concern: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

Conditions that could raise a security concern and may be disqualifying include:

a. The exercise of dual citizenship;

b. Possession and/or use of a foreign passport;

c. Military service or a willingness to bear arms for a foreign country;

d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;

e. Residence in a foreign country to meet citizenship requirements;

f. Using foreign citizenship to protect financial or business interests in another country.

g. Seeking or holding political office in the foreign country;

h. Voting in foreign elections; and

i. Performing or attempting to perform duties, or other-wise acting, so as to serve the interests of another government in preference to the interests of the United States.

Conditions that could mitigate security concerns include:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;

b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;

c. Activity is sanctioned by the United States;

d. Individual has expressed a willingness to renounce dual citizenship.

GUIDELINE D

Sexual Behavior

The Concern: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress, or reflects lack of judgment or discretion. [i] Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance.

Conditions that could raise a security concern and may be disqualifying include:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;

c. Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

d. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

Conditions that could mitigate security concerns include:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;

b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;

c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;

d. The behavior no longer serves as a basis for coercion, exploitation, or duress.

i The adjudicator should also consider guidelines pertaining to criminal conduct (Guideline J) and emotional, mental, and personality disorders (Guideline 1) in determining how to resolve the security concerns raised by sexual behavior.

GUIDELINE E

Personal Conduct

The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

b. Refusal to complete required security forms, releases, or provide full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with a personnel security or trustworthiness determination.

Conditions that could raise a security concern and may be disqualifying also include:

a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination,

d. Personal conduct or concealment of information that may increase an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail;

e. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency,

f. Association with persons involved in criminal activity.

Conditions that could mitigate security concerns include:

a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress;

f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements, and upon being made aware of the requirement, fully and truthfully provided the requested information;

g. Association with persons involved in criminal activities has ceased.

GUIDELINE F

Financial Considerations

The Concern: An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying include:

a. A history of not meeting financial obligations;

b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;

c. Inability or unwillingness to satisfy debts;

d. Unexplained affluence;

e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

Conditions that could mitigate security concerns include:

a. The behavior was not recent;

b. It was an isolated incident;

c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);

d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;

e. The affluence resulted from a legal source; and

f. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

GUIDELINE G

Alcohol Consumption

The Concern: Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

Conditions that could raise a security concern and may be disqualifying include:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;

b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of alcohol abuse or alcohol dependence;

d. Evaluation of alcohol abuse or alcohol dependence by a licensed clinical social worker who is a staff member of a recognized alcohol treatment program;

e. Habitual or binge consumption of alcohol to the point of impaired judgment;

L Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of a alcohol rehabilitation program.

Conditions that could min : gate security concerns include:

a. The alcohol-related incidents do not indicate a pattern;

b. The problem occurred a number of years ago and there is no indication of a recent problem-,

c. Positive changes in behavior supportive of sobriety;

d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participated frequently in meetings of Alcoholics Anonymous or a similar organization, has abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional or a licensed clinical social worker who is a staff member of a recognized alcohol treatment program.

GUIDELINE H

Drug Involvement

The Concern:

a. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

b. Drugs are defined as mood and behavior-altering substances, and include:

(1) Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens), and

(2) Inhalants and other similar substances.

c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

Conditions that could raise a security concern and may be disqualiffing include:

a. Any drug abuse (see above definition);

b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution,

c. Diagnosis by a credentialed medical professional (e.g., physician, clinical psychologist, or psychiatrist) of drug abuse or drug dependence;

d. Evaluation of drug abuse or drug dependence by a licensed clinical social worker who is a staff member of a recognized drug treatment program;

e. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional. Recent drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will almost invariably result in an unfavorable determination.

Conditions that could mitigate security concerns include:

a. The drug involvement was not recent;

b. The drug involvement was an isolated or aberrational event;

c. A demonstrated intent not to abuse any drugs in the future;

d. Satisfactory completion of a prescribed drug treatment program, including rehabilitation and aftercare requirements, without recurrence of abuse, and a favorable prognosis by a credentialed medical professional.

GUIDELINE I

Emotional, Mental, and Personality Disorders

The Concern: Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability, or stability. A credentialed mental health professional (e.g., clinical psychologist or psychiatrist), employed by, acceptable to or approved by the government, should be utilized in evaluating potentially disqualifying and mitigating information fully and properly, and particularly for consultation with the individual's mental health care provider.

Conditions that could raise a security concern and may be disqualifying include:

a. An opinion by a credentialed mental health professional that the individual has a condition or treatment that may indicate a defect in judgment, reliability, or stability;

b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a condition, e.g., failure to take prescribed medication;

c. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;

d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

Conditions that could mitigate security concerns include:

a. There is no indication of a current problem-,

b. Recent opinion by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured, under control or in remission, and has a low probability of recurrence or exacerbation;

c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

GUIDELINE J

Criminal Conduct

The Concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

a. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

b. A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

a. The criminal behavior was not recent;

b. The crime was an isolated incident,

c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;

d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur-,

e. Acquittal;

f. There is clear evidence of successful rehabilitation.

GUIDELINE K

Security Violations

The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern and may be disqualifying include:

a. Unauthorized disclosure of classified information;

b. Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns include actions that:

a. Were inadvertent;

b. Were isolated or infrequent;

c. Were due to improper or inadequate training;

d. Demonstrate a positive attitude towards the discharge of security responsibilities.

GUIDELINE L

Outside Activities

The Concern: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

Conditions that could raise a security concern and may be disqualifying include any service, whether compensated, volunteer, or employment with:

a. A foreign country;

b. Any foreign national;

c. A representative of any foreign interest;

d. Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

Conditions that could mitigate security concerns include:

a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

GUIDELINE M

Misuse of Information Technology Systems

The Concern: Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

a. Illegal or unauthorized entry into any information technology system;

b. Illegal or unauthorized modification, destruction, manipulation or denial of access to information residing on an information technology system;

c. Removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

d, Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Conditions that could mitigate security concerns include:

a, The misuse was not recent or significant;

b. The conduct was unintentional or inadvertent;

c. The introduction or removal of media was authorized;

d. The misuse was an isolated event;

e. The misuse was followed by a prompt, good faith effort to correct the situation.

INVESTIGATIVE STANDARDS FOR BACKGROUND INVESTIGATIONS

FOR

ACCESS TO CLASSIFIED INFORMATION'

A. INTRODUCTION

The following investigative standards have been established for all United States Government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information (SCI) and Special Access Programs (SAPs), and constitute the investigative basis for final clearance determinations. However, nothing in these standards prohibits the Department of Defense from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

B. THE THREE STANDARDS

There are three standards (Table I summarizes when to use each one):

1. The investigation and reinvestigation standard for access to CONFIDENTIAL and SECRET (including all SECRET-level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish SAPs by Section 4.4 of Executive Order 12958);

2. The investigation standard for access to TOP SECRET (including TOP SECRET SAPs) and SCI; and

3. The reinvestigation standard for continued access to the levels listed in subsection B.2, above.

C. EXCEPTIONS TO PERIODS OF COVERAGE

Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the subject's 18th birthday to the present or to two years, whichever is longer.

Comment: However, no investigation shall be conducted prior to an individual's 16th birthday. Additionally, lack of coverage in any investigative category shall be compensated for through other investigative means.

Italized type is used to amplify the standards in certain areas for implementation within DoD.

D. **EXPANDING INVESTIGATIONS**

Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

E. **TRANSFERABILITY**

Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

F. **BREAKS IN SERVICE**

If a person who requires access has been retired or separated from U.S. Government employment for less than 24 months and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated SF 86 *(or EPSQ)* and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of this Regulation.

G. **THE NATIONAL AGENCY CHECK (NAQ)** The NAC is a part of all investigations and reinvestigations.

Comment: The scope for the NAC is five years or to age 18, whichever is the shorter period.

At a minimum, it consists of a review of the following-

1. Investigative and criminal history files of the FBI, including a technical fingerprint search;

a. FB11HQ has on file copies of investigations conducted by the FBI. TheFB11HQ check consists of a review of files for information of a security nature and that developed during applicant-type investigations.

b. FBI17D check (excluding EATNACs) is based upon a technical fingerprint search that consists of a classification of the subject's fingerprints and a comparison with fingerprint cards submitted by law enforcement activities. If the fingerprint card is not classifiable, a "name check only" of these files is automatically conducted.

2. OPM's Security/Suitability Investigations Index (SU): *The files of OPM contain the results of investigations conducted by OPM under Executive Order 10450, those requested by the NRC, the DOE, and those requested since August 1952 to serve as a basis for "Q" clearances.*

Additionally, personnel security adjudicative determinations rendered by other federal agencies are contained in the SII. OPM S11 records will be checked on all subjects of DoD investigations.

3. Defense Clearance and Investigations Index (DCH): *The DCII data base consists of an alphabetical index of personal names and impersonal titles that appear as subjects, co-subjects, victims, or cross-referenced incidental subjects, in investigative documents maintained b - v DoD criminal, counterintelligence, fraud, and personnel security investigative activities. Additionally, personnel security adjudicative determinations are maintained by subject in the DCII. DCII re cords will be checked on all subjects of DoD investigations.*

4. Such other national agencies (e.g., CIA, INS) appropriate to the individual's background.

a. *Central Intelligence Agency (CIA . The CIA maintains the following records:*

(1) Directorate of Operations (CIA-DO/1MS) maintains the Foreign Intelligence Counterintelligence database. This database shall be checked for all foreign nationals residing outside the U.S. requiring access to classified infor7nation (i.e., LAA). If the requester provides complete personal identifying information (complete name, date of birth, place of birth, and citizenship), all alien co-subjects (on SSBIs) residing outside the U.S. are also checked In addition, this database shall be queried on the subject any time there is a counterintelligence concern raised during the conduct of the PSI.

(2) Office of Security (CJA-OS) maintains information on present and former employees, including members of the Office of Strategic Services (OSS), and applicants for employment. These files shall be checked if subject has been an employee of the CIA or when other sources indicate that the CIA may have pertinent information.

b. Immigration and Naturalization Service (I&NS :The files of I&NS contain (or show where filed) naturalization certificates, certificates of derivative citizenship, all military certificates of naturalization, repatriation files, petitions for naturalization and declarations of intention, visitor's visas, and records of aliens (including government officials and representatives of international organizations) admitted temporarily into the United States. I&NS records are checked when the subject is:

(])An alien in the U.S., or

(2) A naturalized citizen whose naturalization has not been verified, or

(3) An immigrant alien, or

***(4) A U.S. citizen who received derivative citizenship through the naturalization** of one or both parents provided that such citizenship has not been verified in a prior investigation.*

c. State Department :The State Department maintains the following records:

(1) Security Division files contains information pertinent to matters of security, violations of security, personnel investigations pertinent to that agency, and correspondence files from 1950 to date. These files are checked on all former State Department employees.

(2) Passport Division files shall be checked if subject indicates U.S. citizenship due to birth in a foreign country of American parents. This is a check of State Department Embassy files to determine if subject's birth was registered at the U.S. Embassy in the country where helshe was born. Verification of this registration is verification of citizenship.

d. Military Personnel Record Center: Files are maintained by separate departments of the Armed Forces, General Services Administration, and the Reserve Records Centers. They consist of the master personnel records of retired, separated, reserve, and active duty members of the Armed Forces.

***Comment:** Military requesters must review service records of any active duty member at the time the investigation is requested. Unfavorable information must be recorded on the investigative request form. Review ofprior military service records is to be conducted by the investigating agency through the Defense Manpower Data Center databases or the Military Personnel Record Center files, as appropriate.*

e. Treasury Department: The files of Treasury Department agencies (Secret Service, Internal Revenue Service, and Bureau of Customs) shall be checked only when available information indicates that an agency of the Treasury Department may be reasonably expected to have pertinent information.

f *7hefiles of other agencies such as the National Guard Bureau, etc. shall be checked when pertinent to the purpose for which the investigation is being conducted.*

H. NATIONAL AGENCY CHECK WITH LOCAL AGENCY CHECKS AND CREDIT CHECK(NACLC)

1. Applicability: The NACLC applies to the investigations and reinvestigations conducted to determine eligibility for access to CONFIDENTIAL and SECRET (including all SECRET level SAPs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by section 4.4, E.O. 12958).

2. For Reinvestigations: When to Reinvestigate. The reinvestigation may be initiated at any time following completion of, but not later than ten years for SECRET (15 years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation including when there has been a break in service.).

3. Investigative Requirements:

a. Completion of Forms. Completion of SF 86 *(or EPSQ)* including applicable releases and supporting documentation;

b. National Agency Check. Completion of a NAC.

Comment: For Secret and Confidential periodic reinvestigations, fingerprint cards are not required if there is a previous valid technical check of the FBI.

c. Financial Review: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

d. Date and Place of Birth: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation, and a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

Comment: Verification of date and place of birth by sighting an original or certified copy of a birth certificate or other acceptable documentation should nor7nally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance.

e. Local Agency Checks: As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last five years, and, if applicable, of the appropriate agency for any identified arrests.

f. Expanding the Investigation. The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

1. SINGLE SCOPE BACKGROUND INVESTIGATION (SSBI)

1. Applicability : The initial investigation for access to TOP SECRET (including TOP SECRET SAPs), SCI, and occupancy of a critical sensitive position.

2. Investigative Requirements:

a. Completion of Forms. Completion of SF 86 *(or EPSQ),* as appropriate, including applicable releases and supporting documentation;

b. National Agency Check. Completion of a NAC.

c. National Agency Check for the Spouse or Cohabitant (if applicable - Completion of a NAC, without fingerprint cards, for the spouse or cohabitant.

d. Date and Place of Birth. Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

Comment: Verification of date and place of birth by sighting an original or certified copy of a birth certificate or other acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the DD 1879 should be annotated to this effect.,

e. Citizenship. For individuals born outside the United States, verification of U.S. citizenship directly from the appropriate registration authority; verification of U.S. citizenship or legal status of foreign-born immediate fan-Lily members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

Comment: Verification of citizenship by sighting of acceptable documentation should normally be accomplished by the requester prior to initiating the request for investigation. When such documentation is not readily available, investigative action may be initiated with the understanding that said documentation must be provided prior to the issuance of a clearance. If a variance or discrepancy in the documentation provided exists, the DD 1879 should be annotated to this effect. For individuals born outside the U.S., the investigating agency will verify citizenship directl yfrom the appropriate registration authority and also, verify U.S. citizenship or legal status of foreign-born immediate family members.

Acceptable proofs of citizenship are as follows:

(1) For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office. The only exception is a state or other jurisdiction that does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable.

(2) A delayed birth certificate is one created when a record was filed more than one year after the date of birth. Such a certificate is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include: baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of birth. Other documentary evidence can be early census, school, or family bible records, newspaper files, or insurance papers.

(3) All documents submitted as evidence of birth in the United States shall be original or certified documents. Uncertified copies are not acceptable.

(4) If the individual claims citizenship by naturalization, a certificate of naturalization shall be submitted.

(5) If citizenship was acquired by birth abroad to a U. S. citizen parent or parents, the following are acceptable evidence:

(a) A Certificate of Citizenship issued by the Immigration and Naturalization Service (I&NS); or

(b) A Report of Birth Abroad of *a Citizen of the United States* of *America (Form FS-240); or*

(c) A Certificate of *Birth (For7n FS-545 or DS-1350).*

(d) A passport or one in which the individual was included will be accepted as proof of citizenship.

f. Education. Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education was a primary activity of the subject during the most recent three years.

Comment: Corroboration of education within the scope of investigation shall normally be accomplished by the requester prior to the initiation of the request for investigation. If all education is outside of the investigative scope, the last education above high school level will be verified.

9. Employment. Verification of all employments for the past seven years; personal interviews of sources (supervisors, coworkers, Or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding 60 days; verification of all prior federal and military service, including type of discharge. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments. However, each duty location must be individually listed.

Comment: *For Federal employees, all service within one agency of the Federal Government will be considered as one employment, regardless 9f assignment. However, each duty location must be individually listed.*

h. References. Four references, of whom at least two are developed; to the extent praeticable, all should have social knowledge of the subject and collectively span at least the last seven years.

i. Former Spouse. An interview of any former spouse divorced within the last ten years.

j. Neighborhoods, Confirmation of all residences for the last three years through appropriate interviews with neighbors and through records reviews.

Comment: The SSBI standard for neighborhoods allows an investigative entity sufficient flexibility to meet the standard, provided that a reasonable effort is made to obtain coverage within the investigative period and the lack of coverage in any investigative category should be compensated for through other investigative means.

k. Financial Review. Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

1. Local Agency Checks. A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and /or attended school for six months or more, including current residence regardless of duration. If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.

m. Public Records. Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.

n. Subject Interview. A subject inter-view, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

o. Polygraph (only in agencies with approved personnel security polygraph programs). In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

3. Expanding the Investigation. The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

J. SINGLE SCOPE BACKGROUND INVESTIGATION - PERIODIC REINVESTIGATION (SSBI-PR)

1. Applicability . Applies to reinvestigations for access to TOP SECRET (including TOP SECRET SAPs), SCI.

Comment: Also, applies to eligibility for occupancy of a critical sensitive position.

2. When to Reinvestigate. The reinvestigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation (see Table 2).

Comment: The investigation will cover the most recent five year period or the period since the last investigation, whichever is shorter.

3. Reinvestigate Requirements. Reinvestigate requirements are as follows:

a. Completion of Forms. Completion of SF 86 *(or EPSQ)*, as appropriate, including applicable releases and supporting documentation.

b. National Agency Check. Completion of a NAC (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).

c. National Agency Check for the Spouse or Cohabitant (if applicable). Completion of a NAC, without fingerprint cards, for the spouse or cohabitant. The NAC for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.

d. Employment. Verification of 0 employments since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employment of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

Comment: For Federal employees, all service within one agency of the Federal Government will be considered as one employment, regardless of assignment.

e. References. Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practicable, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

f. Neighborhoods. Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Confirmation of current residence regardless of length.

Comment: The SSBI-PR standard for neighborhoods allows any investigative entity sufficient flexibility to meet the standard, providing that a reasonable effort is made to obtain coverage within the investigative period and that lack of coverage in any investigative category should be compensated for through other investigative means.

g. Financial Review.

1) Financial Status. Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) Check of Treasury's Financial Database. Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign banks and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

h. Local Agency Checks. A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. If no residence, employment, or education exceeds six months, local agency checks should be performed as deemed appropriate.

i. Former Spouse. An inter-view with any former spouse unless the divorce took place before the date of the last investigation or reinvestigation.

Comment: An interview will be conducted with any former spouse whose divorce from Subject took place after the date of the last investigation or reinvestigation (regardless of how long the interval).

j. Public Records. Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

k. Subject Interview. A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject inter-views may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

4. Expanding the Reinvestigation. The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

K. INVESTIGATIVE STANDARDS FOR TENTORARY ELIGIBILITY FOR ACCESS

1. Introduction. Minimum investigative standards, implementing Section 3.3 of Executive Order 12968, are established for all DoD military personnel, civilian employees, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other personnel who require access to classified information before the appropriate investigation can be completed and a final determination made,

2. Temporary Eligibility for Access . In exceptional circumstances where official functions must be performed prior to completion of the investigation and adjudication process, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

a. CONFIDENTIAL and SECRET Levels. As a minimum, such temporary eligibility requires completion of the SF 86 (or *EPSQ)*, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, a DCII check, and submission of an expedited request for an NACLC.

b. TOP SECRET and SCI Levels For someone who is the Subject of a Favorable Investigation Not Meeting the Investigative Standards for Access at Those Levels. As a minimum, such temporary eligibility requires completion of the SF 86 (or *EPSQ)*, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and expedited submission of a request for an SSBL

c. TOP SECRET and SCI Levels For someone who is Not the Subject of a Current, Favorable Personnel or Personnel-Security Investigation of Any Kind. As a minimum, such temporary eligibility requires completion of the SF 86 (or *EPSQ)*, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited SSBI, and completion and favorable review by the appropriate adjudicating authority of relevant crirninal history and investigative records of the FBI and of information in the Security/Suitability Investigations Index (SIT) and the DCIL

d. Additional Requirements by Agencies. Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified in formation necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, no additional requirements shall exceed the common standards for background investigations as contained in this Regulation. Temporary eligibility for access is valid only at the agency granting it and at other agencies that expressly agree to accept it and acknowledge understanding of its investigative basis. Where temporary eligibility for access is granted under the provisions of this section, or where the determination of eligibility for access is conditional, the fact of such temporary or conditional access shall be conveyed to any other agency that considers affording the subject access to its information.

DECISION TABLES

TABLE 1: WHICH INVESTIGATION TO REQUEST

If the requirement is for	And the person has this access	Based on this investigation	Then the investiation required is	Using standard
CONFIDENTIAL SECRET	none	none	NACLC	H
	CONFIDENTIAL SECRET; "L"	out of date NAC, ENTNAC, NACIC, NACLC, BI, SBI, or SSBI		
TOPSECRET, SCI:	none	none	SSBI	I
	none; CONF, SEC; "L"	current or out of date NAC, ENTNAC, NACIC, NACLC, BI, SBI		
	TS, SCI; "Q"	out of date SSBI	SSBTPR	I

TABLE 2: REINVESTIGATION REQUIREMENTS

If the requirement is for	And the age of the investigation is	Type required if there has been a break in service or employment of		*Type required if there has been a break in access (no access1lower level* of *access) but remains in military service, federal service, or with same employer in industry*
		0-23 mos.	24 mos. or more	
CONFIDENTIAL	0 to 14 yrs. 11 mos.	None	NACLC	*None*
	15 yrs. or more	NACLC-PR	NACLC	*NACLC-PR*
SECRET	0 to 9 yrs. 11 mos.	None	NACLC	*None*
	1 O yrs. or more	NACUC-PR	NACLC	*NACLC-PR*
TOP SECRET, SCI	0 to 4 yrs. 11 mos,	None (Note 2)	SSBJ	*None*
	5 yrs. or more	SSBI-PR	SSBI	SSBI-PR

NOTE 1: The NACLC investigative and reinvestigate requirement for Secret and Confidential access will begin January 1, 1999. Personnel with an existing NACIENTNAC completed prior to January 1, 1999 and who have prior security clearance eligibility, will not require a NACLC to maintain their Secret or Confidential clearance. However, personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and no prior security

clearance eligibility, will require a NACLC for issuance of a Secret or Confidential clearance, regardless of the age of the investigation.

NOTE 2: As a minimum, review an updated SF-86 and applicable records. A reinvestigation SSBI-PR is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 1296&

Implementation of the NACLC

- Any National Agency Check (NAC) or Entrance NAC (ENTNAC) submitted for a Secret or Confidential clearance and opened by DSS prior to January 1, 1999, will be eligible for issuance of a security clearance.

- Any Secret/Confidential clearance request opened by DSS after January 1, 1999 will be run as a NACLC, this includes enlisted and officer accessions. Requests not indicating the investigation is for a clearance will continue to be run as a NAC or ENTNAC.

- Personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and who have a prior security clearance eligibility, will not require a NACLC to maintain their Secret or Confidential clearance. However, personnel with an existing NAC/ENTNAC completed prior to January 1, 1999 and no prior security clearance eligibility, will require a NACLC for issuance of a Secret or Confidential clearance, regardless of the age of the investigation.

- An NACIC and ANACI will serve as the basis for issuance of Secret or Confidential clearances for civilian employees.

Attachment 3

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-60M

August 22, 2000

COMMAND, CONTROL, COMMUNICATIONS. AND INTELLIGENGINCE

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRFCTOR~ ADMI341STRATION AND MANAGEMFNT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF TIAF- DOD FIELD ACTIVITTES

SUBJECT: Personnel Security Clearance Investigations

The Deputy Secretary accepted, on March 31, 2000, the recommendations of the Overarching Integrated Process Team (OIPT) to eliminate the periodic reinvestigation (PR) backlog by the end of FY2002. This memorandum implements the Deputy Secretary's direction to distribute, effective October 1, 2000, the personnel security clearance investigation workload between the Defense Security Service (DSS) and the Office of Personnel Management (OPM). Attachment I depicts the workload distribution. In summary, initial investigations for a Secret/Confidential clearance and periodic reinvestigations (PRs) for military personnel shall be forwarded to the OPM. Military accession investigations, except for the Army personnel, will be sent to OPM. Army military accessions will continue to be sent to the DSS. Investigations of civilian and military personnel stationed overseas or who have overseas activity within the scope of the investigation Fire to be sent to DSS- In accordance with prior guidance and except for overseas investigations, all DoD civilian personnel investigations will continue to be sent to OPM. Attachment 2 provides instructions for processing military investigations by OPM. The processing guidance previously issued for civilian personnel remains unchanged.

The success of this aggressive effort requires close monitoring and the commitment of all addressees. In addition to other requirement, the Under Secretary of Defense (Comptroller) (USD(C)) issued a memorandum on June 22, 2000, that asked the Components to appoint a *senior official to oversee the execution of their workload plan.* Within 5 days of the date of this memorandum, request that you identify to me the name of the senior official, preferably at the Assistant Secretary level or Deputy Director for Defense Agencies, who will ensure the needed monitoring and Component commitment to this effort.

The senior Component official is responsible, as a minimum, for developing a Component-level plan, and for monitoring and reporting Component status with respect to the USD(C) spend plan. The plan must address:

- The availability of sufficient funds
- The generation of sufficient workload from field activities in the timelines identified
- Ensuring the quality of submissions so as to preclude rejection and needless delays
- Ensuring the timely adjudication of completed ca3r3

The designated Component senior official is to advise me, within 15 days of the date of this memo, of any known impediments to executing the June 22, 2000 plan issued by the USD(C). Also, provide me with a quarterly report regarding compliance with this plan, to include the tour points mentioned above. This report will be due not later than 15 days after the end of each quarter for FY2001 and FY2002. My office will provide a monthly execution report (Attachment 3) to each Component senior official, and to the Secretary of Defense and Deputy Secretary of Defense.

Other actions:

- I encourage you to have your Inspectors General include compliance with the workload plan as a matter of interest during inspections for FY2001 and FY2002 to preclude recurrence of a PR backlog.

- By the end of FY2002, all active clearances/accesses are to be:

  - based upon a current investigation in accordance with the national standards, or -in-process for an appropriate reinvestigation (i.e., funded with the proper forms submitted).

By September 30, 2002, if a clearance is not based upon a current investigation (or is not in process for a current reinvestigation), or immediately if the position does not support a requirement for a clearance, the clearance must be administratively terminated or downgraded without prejudice to the individual. This does not authorize the removal of any individual from employment because of an overdue investigation. If a bonafide requirement for access to classified information subsequently develops, the clearance can be reinstated immediately even if the investigation is outdated, provided the reinvestigation process has been initiated.

While the above guidance applies to clearances for access to classified information, it is equally important to ensure that other critical positions (e.g. presidential support~ system/network administrators) have current investigations as well.

I am committed to maintaining a viable and robust personnel security program. Ensuring the reliability and trustworthiness of all DoD personnel with access to classified information, other mission critical information and systems, remain- a mission critical requirement.

Arthur L. Money

Attachments

Division of Workload

	SSBI	TS-PR	NACLC	ACCESSIONS
Military	DSS	DSS	OPM*	Army Coast DSS Guard AF Navy OPM Marines
Civilian Industry	OPM* DSS	OPM* OSS	OPM* DSS	

*Investigations on civilian/military personnel currently stationed overseas or who have overseas activity within the scope of the investigation are to be sent to DSS.

Instructions for Processing Military Investigations to OPM

Effective October 1, 2000

Table of Contents

Attachment 2

Processing Instructions

Introduction

This attachment provides instructions for submitting accession and non-accession investigations to the Office of Personnel Management (OPM) for DoD Military Personnel.

This includes the Entrance National Agency Check (ENTNAC) and NAC with Local Agency Checks and Credit check (NACLC). The latter would be for both initial and periodic reinvestigations for SECRET and CONFIDENTIAL clearances.

As of ***October 1. 2000,*** the current automated ENTNAC conducted by DSS will be obsolete. The "new" ENTNAC will consist of a technical search of the FBI criminal indices, (using an FD 258) and the FBI's investigative indices. A check of the Defense Clearance and Investigations Index (DCII) and the Security/Suitability Investigations Index (SIT) will also he accomplished. For the purpose of this 24-month migration period only, all ENTNACS may be submitted to OPM or DSS via FD258 (or LTVESCAN) without a completed SF86/EPSQ. This would include non-U.S. citizens and naturalized citizens who would not be subject to an Immigration and Naturalization Service (INS) check under this scenario. Such ENTNACs may not serve as the basis for issuance of an interim security clearance unless and until the person's U.S. citizenship, as a minimum, has been verified.

All Navy and Air Force accessions and some USMC and Army accessions will be subject to the NACLC. All officer accessions will be subject to a NACLC.

The FBI has projected a 24-hour turnaround time for electronic fingerprint submissions submitted by OPM and DSS. The 24-hour timeframe excludes those National Fingerprint File States and any manual conversion arrest records. OPM's front and back end processing timeliness is *not* included.

DSS will continue to conduct overseas investigations. Investigations on civilian/military personnel currently stationed overseas or who have overseas activity within the scope of the investigation are to be sent to DSS_

OPM requires a submitting office number (SON) when requesting an investigation. To obtain a SON: Complete the PIPS Form 12 and forward it to OPM.

OPM has established a new mailing address for the processing of military investigations. It is:

U.S. Office of Personnel Management
Federal Investigations Processing Center
P.O. Box 700
113 7 Branchton Road
Boyers, PA 16018-0700

Processing Instructions for *ARMY* Military Personnel

Effective October 1, 2000

1. Accession

- No change. All accession investigations (ENTNAC and NACLQ will continue to be sent to DSS. This also includes those SSBIs required by new accessions,
- Automated ENTNAC will be replaced by the "new" ENTNAC (tech check)

- Until fingerprint LIVESCAN equipment is installed at all MEPS locations

- MEPS will:
- For ENTNAC
    - Mail the FD258 fingerprint card to DSS
- For NACLC
    - Mail the FD258 fingerprint card to DSS f6rr initiation of the NAC
    - Recruiter will:
        - Transmit the SF861EPSQ to DSS
        - Mail the Authorization for Release to DSS

- When LIVESCAN is installed
- MEPS will:
    - For ENTNAC
        - Transmit fingerprints via LIVESCAN to DSS
- For NACLC
    - Transmit fingerprints via LIVESCAN to DSS for initiation of the NAC
    - Recruiter will;
        - Transmit the SF96/EPSQ to DSS
        - Mail the Authorization for Release to DSS

11. Non-Accession

• All NACLCs for SECRET/CONFIDENTIAL clearances (except when overseas activity exists) are to be sent to OPM.
• The SF 86/EPSQ (printed paper form with signed release(s)), FD258 fingerprint card (as appropriate), and Agency Use Block information are to be mailed to OPM.
• There is no plan for the Army to support electronic submission of the EPSQ to OPM.

Mail to:

Accession Investigations to DSS
Defense Security Service
Personnel Investigations Center
P.O. Box 18585
ATTN: Records Management Group
Baltimore, MD 21240

Non-Accession Investigations to OPM
U.S. Office of Personnel Management
Federal Investigations Processing Center
P.O. Box 700
1137 Branchton Road
Boyers, PA 16018-0700

Processing for *NAVY* Military Personnel

Effective October 1, 2000

I. Accession

- Navy will submit NACLCs on all accessions
- All accession investigations will be sent to OPM

- Until fingerprint LIVESCAN equipment is installed at all MEPS locations
  - MEPS will:
    & Mail the FD258 fingerprint card to OPM for initiation of the NAC
  - Recruiter will: Mail the SF86/EPSQ (printed paper form with signed release(s)), and Agency Use Block information to OPM OPM will not initiate the NACLC until the release and Agency Use Block information have been received and matched up with the EPSQ

- When LIVESCAN is installed
  - MEPS will:
    - Transmit fingerprints via LIVESCAN to OPM
  - Recruiter will: Mail the SF86/EPSQ (printed paper form with signed release(s)), and Agency Use Block information to OPM
- OPM will **not** initiate the NACLC until the release and Agency Use Block information have been received anti matched up with the EPSQ

II. Non-Accession

All NACLCs for SECRET/CONFIDENTLAL clearances (except when overseas activity exists) are to be sent to OPM. The SF WEPSQ (printed paper form with signed release(s)), FD258 fingerprint card (as appropriate), and Agency Use Block information are to be mailed to OPM. There is no plan for the Navy to support electronic submission of the EPSQ to OPM.

Mail to:

U.S. Office of Personnel Management
Federal Investigations Processing Center
P.O. Box 700
113 7 Branchton Road
Boyers, PA 16018-0700

Attachment 2

Processing Instructions for the *AIR FORCE*, Military Personnel

Effective October 1, 2000

- The Air Force is establishing a separate communications link with OPM to transmit the SF86/EPSQ. Air Force will provide the necessary communications and computer hardware and software to accomplish this as well as the personnel resources to match the EPSQ with the release and agency use block information. Detailed guidance for this process will be provided by the Air Force.

1. Accession

- Air Force will submit NACLCs on all accessions
- All accession investigations will he sent to OPM

- Until fingerprint LIVESCAN equipment is installed at all MEPS locations
- M.EPS will:
  - Mail t1m FD258 fingerprint card to OPM for initiation of the NAC
- Recruiter will: Transmit the SF86 via AFRISS to the Air Force server
  - Mail, fax, or scan the Authorization for Release of Information and Agency Use Block information to the AF staff at OPM.
- OPM will not initiate the NACLC until the release and Agency Use Block information have been received and matched up with the SF86

- When LIVESCAN is installed
- MEPS will:
  - Transmit fingerprints via 1.1 V ENCAN to OFM
- Recruiter will:
  - Transmit the SF86 via AFRISS to the Air Force server
  - Mail, fax, or scan the Authorization for Release of Information and Agency Use Block information to the AF staff at OPM.
- OPM will not initiate the NACLC until the release and Agency Use Block information have been received and matched up with the SF86

II. Non-Accession

- NACLCs for SECRET/CONFIDEN'I'LAL clearances (except when overseas activity exists) are to be sent to OPM in one of two ways;
  - Electronically - SF86 transmitted to the AF server
    - Mail, fax, or scan the Authorization for Release of Information and Agency Use Black information to the AF staff at OPM. The FD258 fingerprint card (as appropriate) must be mailed to the AF staff at OPM.
    - Manually The SF86/EPSQ (printed paper form with signed release(s)), Agency Use Block information, and FD258 fingerprint card (as appropriate) are to be mailed to OPM.

Mail to:

Electronic Submission
U~S. Office of Personnel Management
Federal Investigative Processing Center
P.O. Box 700
ATTN: AF Staff
113 7 Branchton Road
Boyers, PA 16018-0700

Manual Submission
U.S. Office of Personnel Management
Federal Investigations Processing Center
P.O. Box 700
1137 Branchton Road
Boyers, PA 16018-0700

Attachment 2

Processing for *USMC* Military Personnel

Effective October 1, 2000

I. Accessions

- USMC accessions investigations (NACLC and EN FNAC) will be sent to OPM.
- Automated ENTNAC will be replaced by the "new" ENTNAC (tech check)

- Until fingerprint LIVESCAN equipment is installed at all MEPS locations
  - MEPS will:
    - For ENTNAC
    - Mail the FD258 fingerprint card to OPM
  - NACLC
    - Mail the FD258 fingerprint card to OPM for initiation of the NAC
    - Recruiter will:
      - Mail the SF86/EPSQ (printed paper form with signed release(s)), and Agency Use Block information to OPM.
- OPM will not initiate the NACLC until the release and Agency Use Block information have been received and matched up with the EPSQ.

- When LIVESCAN is installed
  - MEPS will:
    - For ENTNAC
      - Transmit fingerprints via LIVESCAN to OPM
  - For NACLC
    - Transmit fingerprints via LIVESCAN to OPM for initiation of the NAC
    - Recruiter will:
      - Mail the SF86/EPSQ (printed paper form with signed release(s)), and Agency Use Block information to OPM.

- OPM will <u>not</u> initiate the NACLC until the release and Agency Use Block information have been received and matched up with the EPSQ.

II. Non-Accession

- All NACLCs for SECRET/ CONFIDENTIAL clearances (except when overseas activities exists) are to be sent to OPM.
- The SF86/EPSQ (printed paper form with signed release(s)), Agency Use Block information, and FD259 fingerprint card (as appropriate) are to be mailed to OPM.
- There is no plan for the Marine Corps to support electronic submission of the EPSQ to OPM.

Mail to:

U-S. Office of Personnel Management
Federal Investigations Processing Center
P.0. Box 700
1137 Branchton Road
Boyers, PA 16018-0700

Attachment 2

This form is to be attached to each Electronic Personnel Security Questionnaire (EPSQ) submitted to OPM for investigation. Note: *The EPSQ is for internal DOD use only, and is pending OMB approval.*

Agency Use Information (SF86)

A Type of Investigation		B Extra Coverage		C Sensitivity Level		D Access		E Nature of Action Code		F Date of Action	Month Day Year
G Geographic Location			H Position Code		I Position Title						
J SON		K Location of Official Personnel Folder		None NPRC At SON	Other Address						Zip Code
L SOI		M Location of Security Folder		None At SOI NPI	Other Address						Zip Code
N OPAC-ALC Number			O Accounting Data and/or Agency Case Number								
P Requesting Official	Name and Title			Signature				Telephone Number ( )		Date	

The following information is requested as part of your EPSQ for an investigative request being sent to OPM. This information will be used to obtain records in order to determine your suitability for employment. Please sign and date this sheet certifying the accuracy of the information you provided.

Subject of Investigation (Identifying Information)

FULL NAME

* If you have only initials in your name, use them and state (IO)
* If you have no middle name, enter "NMN"
* If you are a "JR.", "SR", "II", etc., enter this in the box after your middle name

Last Name	First Name	Middle Name	Jr., II, etc.

Maiden Name Used

List your maiden name and the "To and From" dates of when it was used.

Maiden Name	Month/Year To	Month/Year

Education Degree(s) (Not shown on the EPSQ)

OPM verifies highest degree obtained and degrees pertinent to the position for which this investigation is conducted. Please list education information below for those degrees beyond the 7 year period, not listed on your EPSQ. Use the number "2" in the Code block which represents College/University/Military College.

Month/Year #1 To	Code	Name of School	Degree/Diploma/Other	Month/Year Awarded
Street Address and City (County) of School			State	Zip Code
Month/Year #2 To	Code	Name of School	Degree/Diploma/Other	Month/Year Awarded
Street Address and City (County) of School			State	Zip Code

Appointee/Applicant Signature: **Date:**

August 2000

Instructions for Completing the SF-86 "Agency Use" Block

NOTE: The instructions are a summary of the items that need completed on blocks A-P of the "Agency Use" portion of the SF 86. It represents a brief description only, any specific questions can be addressed by calling OPM-FIPC at *(724) 794-5612.*

A Type of Investigation

Enter the appropriate 3-character code from the chart below that represents the type of investigation and service requested. The first two digits represent the investigation type, and the third digit represents the investigation service. ***Military investigation requests should code block A with an 08B.***

Type of Investigation	35 Day Service	75 Day Service	120 Day Service	Reopen Service	150 Day Service	180 Day Service
SSBI		30B	30C	30D		
SSBI-PR				18D		18F
ANACI		09B		09D		
NACLC		08B		08D		

**Note: Any variation to the service noted above should be made by special request to OPM.*

SSBI: *Single Scope Background Investigation*
SSBI-PR: *Periodic Reinvestigation for Single Scope Background Investigation*
ANACI: *Access National Agency Check with Inquiries*
NACLC: *National Agency Check with Law and Credit*

B Extra Coverage

Enter the appropriate number of the numeric (1-7) and/or alphabetic (A-Z) codes from the chart below that represents the type of extra investigative coverage desired.

Chart codes: O = Optional Coverage S = Standard Coverage N/A = Not Available

Extra Coverage Codes												
Type of Investigation	1 Overseas	2 Credit	3 Advance NAC	4 Mgr/Spvy	5 Public Contact	6 Law Enforce-ment	7 Attach-Ments	II INS	I Spouse INS	L BVS	R Reinvest-igation	Z Criminal Justice Position
SSBI	N/A	S	O	O	O	O	O	S	S	O	O	O
SSBI-PR	N/A	S	O	O	O	O	O	S	S	O	O	O
ANACI	N/A	S	O	N/A	N/A	N/A	O	O	N/A	O	O	O
NACLC	N/A	S	O	N/A	N/A	N/A	O	O	N/A	O	O	O

Code 1 *(Overseas--Subject and Spouse)*: Not available
Code 2 *(Credit)*: Automated scheduling of Credit happens automatically with these case types, no code is necessary.
Code 3 *(Advance NAC)*: The Advance on the National Agency Checks (NAC) consists of an itemized list of the NAC results and or search status. This is notification of item results only, no hardcopy furnished. The Advance NAC Report is sent to the SOI and is available for all case types. If after 30 days from the scheduling date, the NAC(s) are not complete, a NAC Status report will be generated to provide the SOI information on the required NAC items. Place code "3" in Block "B" for this coverage. For more information and sample copies of the reports, contact OPM-FIPC. *There is no charge for this extra service.*

Code 4 (Managerial and Supervisory)
Code 5 (Public Contact)
Code 6 (Law Enforcement)
These codes print instructions to the investigators on the Case Assignment Transmittal (CAT) to provide additional coverage for positions requiring these duties. The extra coverage is specified in the Extra Coverage Section of the

investigator's Handbook. An additional $100 surcharge is added to the case cost for this coverage. Place extra coverage code of "4, 5, or 6" in Block B for this coverage.

Code 7 (Attachments): Enter a "7' in Block B to indicate an attachment to the investigation, such as:
-request for license or certificate verification;
-issue(s) information;
-personnel folder or security file information;
-special handling instructions;
-any other information pertinent to the investigation.

Code H (INS); Automated scheduling of the Immigration and Naturalization Search. Place code "H" in Block B for this coverage.

Code I (Spouse INS): Automated scheduling of the Immigration and Naturalization Search for the subject of investigations' spouse. Place code "I" in Block B to request this coverage.

Code L (BVS): Automated scheduling of the Birth Verification at State BVS. Place code "L" in Block B to request this coverage.

Code R (Reinvestigation): This code by-passes the administrative edits resident in PIPS that requires the appropriate level of case type/sensitivity/*access*. Place code "R" in Block B to indicate a reinvestigation,

Code Z (*Criminal Justice Position*): This identifies a Criminal Justice Position that arc exempt from the FBI user fees. Place code "Z" in Block B if the subject is in a Criminal Justice Position.

C **Sensitivity Level**	

Enter in the first space one of the following codes representing the sensitivity level of the position requiring the investigation.

CODE	LEVEL
2	Noncritical-Sensitive
3	Critical-Sensitive
4	Special-Sensitive

Enter "C" in the second space for Computer -ADP position- If not a Computer -ADP position, leave the block blank.

D **Access**	

Enter the appropriate code from the chart below to show the type of security clearance/access the position requires or will require.

CODE	LEVEL
0	Not Required
I	Confidential (Executive Order 12968)
2	Secret (Executive Order 12968)
3	Top Secret (Executive Order 12968)
4	Sensitive Compartmented Information (DCID 1/14)
5	Q-Sensitive (Atomic Energy Act)
6	Q-Non-Sensitive (Atomic Energy Act)
7	L (Atomic Energy Act)
8	Other (specify other security clearance under extra coverage Item B. Code 7)

E Nature of Action Code	

If the person is being investigated for a military accession or military non-accession Secret/Confidential position, enter "MIL". If the person being investigated is a Federal employee or applicant, enter the 3-digit code showing the Nature of Action taken or to be taken for the position requiring the investigation (the same action code as used on the SF-52). If your agency did not use FPM Supplement 296-33 coding, enter "000". If the person being investigated is a contract employee, enter "CON". If the investigation is being requested due to adding access to a current position leave this block blank.

E Date of Action	

Enter the effective date (Month/Day/Year) of the action requiring the investigation. If the action has not been taken, leave the block blank.

G Geographic Location	

Enter the 9-digil "Worldwide Geographic Location Code", showing the actual location of the duty station for the position. The Location Code is an OPM Central Personnel Data File (CPDT') requirement that must be entered on the ST-57 and SF-50 for certain personnel actions, This is a GSA Publication (4/87). *If unknown, leave the block blank.*

H Position Code	

Enter the appropriate alphabetic code from the chart below. If none of the codes apply leave the block blank.

CODE	POSITION
A	Congressional Staff
B	Investigator
C	Astronaut
D	Fellow Programs
E	White House
F	SES/15 (or equivalent)
G	Special/Confidential Assistants (GS/13 and above)
H	Child Care Provider

I Position Title	

Enter the title of the position for which the investigation is being requested. If the person being investigated is a contractor employee, enter "contractor".

J SON	

Enter the 4 character Submitting Office Number (SON); if the Security Office is the Submitting Office, enter the Security Office Identifier (SOI) code. (To obtain a SON: Complete PIPS Form 12 and forward it to OPM).

K Location of Official Personnel Folder		None	Other Address	Zip Code
		NPRC		
		At SON		

Check the correct box that gives us the location of the OPF. Check only one box.

NONE: If the person has never been a Federal employee
NPRC: If the OPF is at the National Personnel Records Center
At SON: If the OPF is at the Submitting Office
OTHER ADDRESS: If the OPF is at any other location (for example, the SOI), furnish the address.

L SOI	

Enter the 4 character Security Office Identifier (SOI). Submitting Offices should contact their Security Office to determine the correct SOL

M Location of Security Folder		None	Other Address	Zip Code
		At SOI		
		NPI		

Check the correct box that identifies the location of the Security folder. Check only one box.

NONE: If there is no security file at your agency

AT SOL If there is a security file at your agency, and it should be reviewed.

NPI: If there is a security file at your agency, but it contains no *pertinent information.*

OTHER ADDRESS: If your agency's security file should be reviewed and it is not at the SOI, furnish the address.

N SOPAC-ALC Number	

For military investigation requests of the NACLC, enter "DSS-MIL". For civilian submissions of the SSBJ, SSBI-PR and NACLC, enter "DSS-CIVL". For Civilian submissions of NACI and ANACI's enter your agency's ALC assigned by OPM for use in the manual billing system. Contact OPM-FIPC at (724) 794-5612 for additional billing information.

O Accounting Data and/or Agency Case Number	

You may enter your agency data for internal use. Up to 25 characters may be entered in this block. (The information you enter will be printed on documents used to close the case to your agency.) If your agency does not need this information, leave the block blank.

P Requesting Official	Name and Title	Signature	Telephone Number 0	Date

Enter the name, title, and the signature of official requesting the investigation; the date, and the commercial telephone number, including area code. This is the person OPM will contact concerning specific case related submission problems.

*(SON label/code:)*_____

U. S. Office of Personnel Management
Investigations Service
Federal Investigations Processing Center
PO Box 618
Boyers, PA 16018-0618
Commercial (724) 794-5612 FAX (724) 794-289

SUBMITTING OFFFICE NUMBER (SON) AUTHORIZATION AND AMENDMENT FORM

ATTENTION: PERSONNEL OFFICER

OPM authorizes an SON for each Personnel Office that submits investigation requests and to make case status requests. The SON data is used to mail a variety of investigative notices, and to contact a submitting office to clarify information that may otherwise delay an investigation. OPM-FIPC must have current information on:

- ☑ Agency name and mailing address; and
- ☑ Name, position, and phone numbers of a contact person.

To request an SON or advise OPM of SON changes, complete the necessary items on the form below. Mail or fax the completed form to the address on the top of this form, attention Program Services Office (PSO). For additional information and/or assistance, call OPM-FIPC, PSO at (724) 794-5612.

1. **SON:**_____ **[ ] Check this block if requesting a new SON**

2. **SOI:**_____

3. **[ ] Change/add Online Payment And Collection (OPAC) Agency Location Code (ALC):** _____

   Billing Address: _____

   _____

   City: _____ State: _____ Zip Code: _____

   Contact Name: _____ Phone: (_____) _____ - _____ Extension: _____

4. **[ ] Change/add Agency Name/Address:**

   Agency Name: _____

   Address: _____

   City: _____ State: _____ Zip Code: _____

5. **[ ] Add Contact Person:**

   Name: _____

   Position: _____

6. **[ ] Delete Contact Person:**

   Name: _____

   Name: _____

7. **[ ] Change/add SON Contact telephone numbers:** Commercial: (_____) _____ - _____ Extension: _____

This form should be duplicated as needed

FIPS Form 12 (Revised February 1999)
Attachment 2

Instructions for Completing Finger Print Hard Cards (FD-258)
for Manual or Electronic Submission to DSS or OPM

The following data must be entered or the investigation will be returned:

- Name [Full name (Last, First, Middle)]
- AKAs [Full name (Last, First, Middle)]
- ORI - Army accession enter USDISOOOZ all others enter USOPMOOOZ
- Date of Birth
- Sex
- Pace - Indicate one of the following: A, B, 1, U or W [See explanation below]
- Height
- Weight
- Eyes - Indicate one of the following: Black, Brown, Green, Maroon, Blue, Gray, Hazel, Pink, or Unknown
- Hair - Indicate one of the following: Bald, Brown, Sandy, Gray or Partially Gray, Black, Blond or Strawberry, White, Red or Auburn, Unknown
- Place of Birth
- OCA - Leave blank.
- SSN
- Signature of Person Fingerprinted - Leave blank
- Date
- Signature of Official Taking Fingerprints
- Employer and Address - complete for OPM and DSS (DSS needs the SON)
- For OPM; The following information must be entered in the format displayed below:
  SON: MEPS ED 4 followed by the letter "M" ALC: DSS-MIL
  SOL DD70 ACCI: (Optional)
- Armed Forces No. MNU - Enter branch of service (Army, Navy, Air Force, Marines, Coast Guard)
- Reason Fingerprinted - Indicate Enlistment or Officer Candidate

Mail hard cards to:

OPM: IS: Federal Investigations Processing, Center
PO Box 618
1137 Branchton Road
Boyers, PA 16018-06 19

Defense Security Service
Fingerprint Processing Center
P.O. Box 28989
Baltimore, MD 21240-8989

RACE: Enter race of individual being fingerprinted

If Subject is:	Enter Code
Chinese, Japanese, Filipino, Korean, Polynesian Indian. Indonesian, Asian Indian, Samoan or any other Pacific Islander	A
A person having origins in any of the black racial Groups of Africa	B
American Indian, Eskimo, or Alaskan native, or a person having Origins in my of the 48 contiguous states of the United States or Alaska who maintains cultural identification through tribal Affiliation of community recognition	I
Of indeterminable race	U
Caucasian, Mexican. Puerto Rican, Cuban, Central or South American, or other Spanish culture or origin, regardless or race	W

Attachment 2

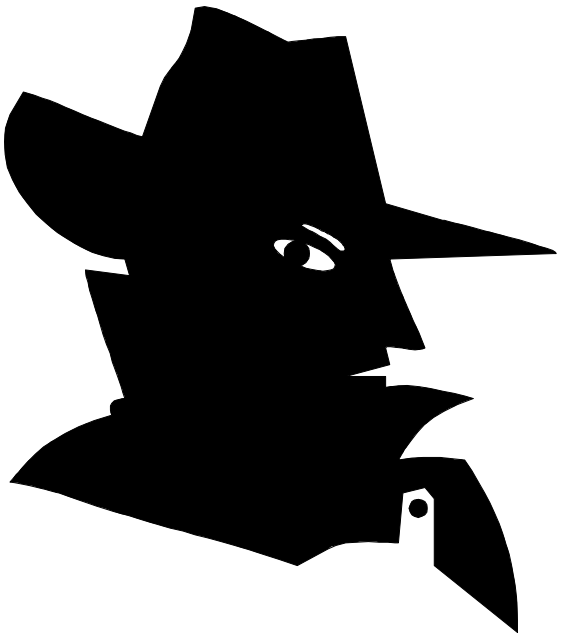
RECENT ESPIONAGE CASES

Summaries and Sources

July 1997

Defense Security Service
Training Office
881 Elkridge Landing Road
Linthicum, MD 21090

Table of Contents



Recent Espionage Cases

Summaries and Sources

In compiling the following short summaries we have intended to include all espionage cases reported in the public media or in unclassified sources which have occurred in the United States since 1975, or which have involved U.S. citizens abroad during the same time span. As events occur, we will continue to update this publication with information from unclassified sources. A number of these case summaries were first published by U.S. Air Force Office of Special Investigations, Quarterly Counterintelligence Digest, Summer 1982. In addition, we have included information from the CIA, FBI, and DIA as appended to the published Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate (April 16-25, 1985). Our information also has been supplemented by the Naval Investigative Service Command's informative summaries published in *Espionage*, 1989.

****

Although it has been asserted in the press that the sharp increase in prosecutions for espionage from 1975 onward was the result of policy changes, it should be noted that “spying” against the United States has been a continuing phenomenon, particularly during the “Cold War” and East-West confrontation.

In fact, at least ten well-publicized events occurred in the mid-60s, which included the damaging defection of Mitchell and Martin (1960), the suicide of Soviet collaborator Jack Dunlap (1963), and the arrests of Johnson and Mintkenbaugh (1964), William Whalen (1966), and John Butenko (1964). Three major cases emerged in the early '70s: Air Force MSG Raymond G. DeChamplain, arrested July 1971 in Bangkok for attempting to pass documents to Soviet embassy staff; Air Force Sgt. Walter T. Perkins, apprehended in October 1971 with classified material which he intended to pass on to the KGB in Mexico; and Sgt. James D. Wood, who was arrested July 1973 in New York as he attempted to transmit documents to a first secretary of the Soviet Embassy.

Nevertheless, the period from about 1968 to 1975 can be seen as a watershed in the history of contemporary espionage—a period of relative calm prior to the escalating frequency of these events in the late '70s and the mid 1980s. Thus we begin our listing of “recent” cases with the year 1975; not denying the fact that espionage events prior to that time bear many of the same characteristics in terms of motivations, *modus operandi*, and contributing factors leading to personal betrayal and the compromise of national security. Following 1989, and with the beginning of the post-Cold War era, the frequency of reported classic espionage events appeared to diminish. However, five significant cases were tallied against 1993. Those who were beginning to think that espionage is out of date and that the foreign intelligence threat is over were hit by a bombshell with news reports of the Ames case and its deadly consequences in early 1994. Another CIA employee and a senior FBI agent both were arrested in 1996 for selling highly classified information to the Russians.

The case summaries conclude with summary bar charts on the number of new cases reported each year and on the types of cases reported.

1975 - SADAG K. DEDEYAN, an employee of the Johns Hopkins Applied Physics Laboratory who was cleared for access to classified information, and a relative, **SARKIS O. PASKALIAN**, were arrested in 1975. Disregarding regulations, Dedeyan brought home a Top Secret document on NATO defenses to work on. Paskalian, who had been recruited and trained by the KGB in 1962, surreptitiously photographed the document and allegedly sold the film to Soviet agents for a reported sum of $1,500. Dedeyan was charged with failing to report the illegal photographing of national defense information. Paskalian was charged with conspiring with Soviet agents to gather and transmit national defense information. Dedeyan was convicted and sentenced to three years. Paskalian pleaded guilty to espionage and was sentenced to 22 years.

Washington Post, 28 Jun 1975, "2 Arrested by FBI On Spying Charges "
"Relative Duped Him on Spy Photographs, Accused Man Says"
"Paskalian: Choreographer, Merchant"
New York Times, 28 Jun 1975, "2 Held in Plot to Spy for Soviets on NATO.

***

1976 - EDWIN G. MOORE II, a retired CIA employee, was arrested by the FBI in 1976 and charged with espionage after attempting to sell classified documents to Soviet officials. A day earlier, an employee at a residence for Soviet personnel in Washington, D.C. had discovered a package on the grounds and turned it over to police, fearing it was a bomb. The package was found to contain classified CIA documents and a note requesting that $3,000 be dropped at a specified location. The note offered more documents in exchange for $197,000. Moore was arrested after picking up what he thought to be the payment at a drop site near his home. A search of his residence yielded ten boxes of classified CIA documents. Moore retired from the CIA in 1973, and although financial gain was a strong motivational factor leading to espionage, it is known that he was disgruntled with his former employer due to lack of promotion. Moore pleaded not guilty by reason of insanity, but was convicted and sentenced to 15 years in prison. He was granted parole in 1979.

Washington Post, 13 Apr 1977, "Thought He was on Assignment for CIA"
25 Apr 1977, "Trial of Ex-Agent..."
6 May 1977, "Moore Guilty of Trying to Sell CIA Files"

***

1977 - IVAN ROGALSKY, a former Soviet merchant seaman admitted to the U.S. as a political refugee, was arrested in New Jersey on 7 January after receiving a classified document from a cleared employee of RCA Research Center. The employee, who worked on communications satellite and defense projects, had agreed to work under FBI control after first being approached by Rogalsky. The ex-seaman had earlier asked the RCA employee for unclassified information about the space shuttle program. A second secretary of the Soviet Mission to the United Nations, **YEVEGENY P. KARPOV**, was named as a co-conspirator. Karpov had been suspected of being a KGB officer by the FBI. According to later press reports, Rogalsky was not tried due to questions regarding his sanity. He claimed to receive instructions from disembodied voices.

New York Times, 8 Jan 1977, "Soviet Alien Arrested in Jersey on Spy Charges"
9 Jan 1977, "Accused Soviet Spy Known as a Drifter"
16 Jan 1977, "Spy Case Clouds a Russian Holiday"

***

1977- CHRISTOPHER J. BOYCE, an employee of TRW Inc., a California-based Defense contractor, and his friend **ANDREW DAULTON LEE**, were arrested in January 1977 for selling classified

information to the Soviets. Over a period of several months, Boyce, employed in a vaulted communications center, removed classified code material which was passed on to KGB agents in Mexico City by Lee. The scheme, which netted the pair $70,000, was discovered only after Lee's arrest by Mexican police as he attempted to deliver classified material at the Soviet embassy. Film strips marked Top Secret found on Lee by Mexican authorities were turned over to the American officials. Under questioning by Mexican security police and FBI representatives, Lee implicated Boyce who was arrested on 16 January in California. The pair are reported to have seriously compromised the Ryolite surveillance satellite system developed at TRW. Lee was sentenced to life in prison, Boyce to 40 years. In 1980 Boyce escaped from prison and spent 19 months as a fugitive. Following Boyce's second apprehension, his sentence was increased by 28 years.

Robert Lindsey, *The Falcon and the Snowman*, Simon and Schuster, 1979
New York Times, 13 Apr 1977, "Alleged Spy for Soviets Linked to C.I.A"
27 Apr 1977, "Man Said to Admit Spying for Soviets"
22 May 1977, "To Be Young, Rich—and a Spy" by Robert Lindsey
Testimony of Christopher J. Boyce before the Permanent Subcommittee on Investigations, April 1985 (cited in the preface)

***

1978 - RONALD HUMPHREY, an employee of the U.S. Information Agency, and **DAVID TRUONG**, a Vietnamese immigrant, were indicted in early 1978. A search of Truong's apartment at the time of his arrest in January uncovered two Top Secret State Department documents. Humphrey had turned over classified cables and documents to Truong who in turn sent them to the North Vietnamese delegation in Paris via a woman who was a Vietnamese double agent working for the FBI. Testimony indicated that Humphrey supplied documents to Truong in order to obtain the release of his common-law wife and her four children from communist Vietnam. Both Humphrey and Truong were convicted on six counts of espionage on 20 May, and on 15 July each received a 15-year sentence.

Washington Post, 21 May 1978, "FBI Continues Spy Case Investigation"
24 May 1978, "Cables in Spy Case Larded with Gossip"

***

1978 - VALDIK ENGER and **RUDOLF CHERNYAYEV**, both Soviet employees of the UN Secretariat, were arrested by the FBI in New Jersey in May 1978 for accepting classified information on anti-submarine warfare passed by a U.S. Naval officer acting on instructions of the Naval Investigative Service and the FBI. The officer, Navy Lieutenant Commander Art Lindberg, acted as a double agent in a counterintelligence operation called Operation Lemonaid. In August 1977, Lt.Cmdr. Lindberg took a trip on the Soviet cruise ship Kazakhstan. Upon the ship's return to New York, he passed a note to one of the Soviet officers containing an offer to sell information. He was later contacted by telephone by a Soviet agent. During subsequent telephone calls LCDR Lindberg was given contact instructions on the type of information to get and the locations of drop sites where that information could be left and payment money could be found. Naval Investigative Service and FBI agents kept the drop zones under surveillance and later identified the Soviet agents. On 20 May 1978, FBI agents moved into the drop zone and apprehended three Soviets, Enger, Chernyayev and another man, **VLADIMIR ZINYAKIN**, third secretary at the Soviet Mission to the United Nations. Zinyakin avoided arrest due to diplomatic immunity. Enger and Chernyayev, the first Soviet officials ever to stand trial for espionage in the United States, were convicted and sentenced to 50 years in prison. Altogether they paid the Navy officer $16,000 for materials he provided. Enger and Chernyayev were later exchanged for the release of five Soviet dissidents.

New York Times, 21 May 1978, "2 Russians Arrested by F.B.I. for Spying"
Washington Post, 24 Dec 1978, "The Spy Who Came Into It Cold"
Los Angeles Times, 24 May 1979, "Navy Officer 'Drafted' as Counterspy"
Naval Investigative Service Command, *Espionage*, 1989

***

1978 - WILLIAM KAMPILES, a lower echelon CIA employee from March to November 1977, was arrested in August 1978 on charges he stole a Top Secret technical manual on an intelligence surveillance system and later sold it to a Soviet agent in Athens, Greece, for $3,000. Kampiles had resigned from the CIA after being told that he was not qualified for work as a field agent. He then proceeded to Greece where he contacted Soviet representatives. His detection followed receipt of a letter by a CIA employee from Kampiles in which he mentioned frequent meetings with a Soviet official in Athens. On returning to the U.S., Kampiles was contacted by FBI special agents and confessed to an act of espionage. Kampiles maintained that his objective was to become a double agent for the CIA. He was sentenced on 22 December to 40 years in prison.

Washington Post, 23 Aug 1978, "CIA 'Big Bird' Satellite Manual Allegedly Sold to Soviets"
New York Times, 12 Nov 1978 "Spy Trial Focusing on Security in C.I.A."
Washington Post Magazine, 4 Dec 1983, "Spy Rings of One"

***

1979 - LEE EUGENE MADSEN, a Navy Yeoman assigned to the Strategic Warning Staff at The Pentagon, was arrested 14 August for selling classified material to an FBI undercover agent for $700. None of 22 highly classified documents taken by Madsen is known to have fallen into the hands of foreign agents; however, it is believed that he had intended to sell them to organized crime figures dealing in narcotics. Madsen, a homosexual, is quoted as saying that he stole Top Secret documents "to prove...I could be a man and still be gay." On 26 October 1979 he was sentenced to eight years in prison.

Washington Post, 27 Oct 1979, "Sailor Receives 8 Years in Jail"

***

1980 - DAVID H. BARNETT, a CIA officer, was indicted 24 October for having sold to the Soviet Union details of one of the CIA's most successful undercover operations code-named "Habrink." Following a tour of duty in Indonesia between 1967 and 1970, Barnett resigned from the CIA to enter private business. In late 1976, faced with failure and debts of $100,000, he offered to sell classified information to the KGB. Barnett handed over full details of Habrink to the KGB, including CIA information on the Soviet SA-2 surface-to-air missile and the Whiskey class diesel-powered submarine. He also revealed the names of 30 CIA intelligence officers as well as the identities of informants recruited by the CIA. In all Barnett was paid approximately $92,000 by the KGB for information supplied between 1976 and 1977. U.S. agents reportedly spotted Barnett meeting the KGB in Vienna in April 1980; he was questioned by the FBI upon his return to the U.S. Barnett entered a plea of guilty and received an 18-year sentence. He was paroled in 1990.

New York Times, 23 Oct 1980, "Alleged Spy Sought 2nd Post, Aides Say"
30 Oct 1980, "Ex-Agent of C.I.A. Pleads Guilty"
Washington Post, 30 Oct 1980, "Ex-CIA Agent Pleads Guilty to Spying"

***

1980 - RUDOLPH ALBERT HERRMANN, KGB career officer, entered the U.S. illegally with his family from Canada in 1968 and operated as a Soviet agent within the U.S. under the guise of a free-lance photographer. His primary assignment was political information. While Herrmann claimed not to

have recruited Americans for espionage, he admitted to having transmitted sensitive information collected by other spies and to acting as a courier for the KGB. Apprehended by the FBI in 1977, he agreed to operate as a double agent until the operation was terminated in 1980. Herrmann and his family were granted asylum in the United States and have been resettled under a new identity.

New York Times, 4 Mar 1980, "Double Agent Revealed by FBI.
Washington Post, 4 Mar 1980, "Soviet Spy Became a 'Double Agent'
John Barron, *The Inheritor: A Tale of KGB Espionage in America*, 1982.

***

1981 - CHRISTOPHER M. COOKE, deputy commander of an Air Force Titan missile crew, was arrested on 21 May and charged with passing classified information to the Soviets which seriously compromised U.S. strategic missile capabilities during the 1980-81 time frame. On his own volition, Cooke began to phone and visit the Soviet embassy in late 1980 with offers to provide classified information. Cooke's motives were never fully established, but it is reported that he was attempting to establish his credentials with the Soviets for the purpose of academic research. It is also known that he sought employment with the CIA on at least two occasions. Believing that Cooke was part of a larger spy ring, Air Force prosecutors offered him immunity from prosecution for a full disclosure. After being given immunity, Cooke admitted to providing classified defense information to the Soviets. The U.S. Court of Military Appeals ordered his release in February 1982 and Cooke resigned his commission.

Washington Post Magazine, 4 Dec 1983, "Spy Rings of One"

***

1981 - WILLIAM H. BELL, project manager of the Radar Systems Group at Hughes Aircraft in El Segundo, California, and **MARIAN ZACHARSKI**, president of the Polish American Machinery Corporation (POLAMCO), were arraigned in June on espionage charges. Bell had been faced with financial difficulties; Zacharski in reality was an officer of the Polish intelligence service. Under the guise of business activities, and over a period of several months, Zacharski developed a relationship with Bell which resulted in the transfer of Secret documents for more than $150,000. As a result, the "quiet radar" and other sophisticated systems developed at Hughes Aircraft were seriously compromised. On 24 June, Bell was confronted by FBI agents with the fact of his involvement in espionage which had been independently established. He confessed and agreed to cooperate with the FBI in the effort to apprehend Zacharski. On 14 December, Zacharski was convicted of espionage and received a life sentence. Bell, who pleaded guilty, was sentenced to eight years. In June, 1985 Zacharski was "swapped" along with three other Soviet Bloc spies for 25 persons held in Eastern Europe. This case is seen as a classic example of recruitment of cleared U.S. personnel for espionage by hostile intelligence operatives.

DoD Security Institute, *Security Awareness Bulletin*, No. 3-83 June 1983
John Barron, *KGB Today: The Hidden Hand*; Reader's Digest Press 1983
Chicago Tribune, 20 May 1984, "Real-life Spy Tale Robbed of an Ending"

***

1981 - MICHAEL R. MURPHY, a Navy Seaman assigned to the USS *James K. Polk* reportedly made several calls to the Soviet Mission to the United Nations in June 1981 offering to make a deal which he said "would benefit both the Soviets and himself." He was offered immunity from prosecution in exchange for cooperation. A polygraph examination indicated that he had contacted the Soviets three times, but had not passed any information. In August, 1981 Murphy was discharged from the Navy.

***

1981 - JOSEPH G. HELMICH, a former U.S. Army Warrant Officer, was arrested on 15 July at his residence in Jacksonville, Florida, for the sale of U.S. cryptography to the Soviet Union from 1963 to 1966. Helmich served as a crypto custodian in France and at Ft. Bragg, N.C. He initiated contact with USSR Embassy officials in Paris after being faced with severe financial problems. In return for extremely sensitive information related to the KL-7 cryptographic system widely used by the U.S. military, Helmich received approximately $131,000. After being transferred to Ft. Bragg, Helmich continued to provide the Soviets with KL-7 key lists and traveled to both France and Mexico City to rendezvous with his handlers. Helmich came under suspicion in 1964 and was questioned because of his unexplained affluence. He was interviewed again in August 1980 and although admitting he had received $20,000 from Soviet agents, denied he had compromised classified information. In early 1981 he was spotted with Soviet agents in Canada. Eventually Helmich recounted full details of his espionage involvement. On 16 October he was sentenced to life imprisonment.

Washington Post, 16 Jul 1981, "Ex-Army Cryptographer Indicted on Spy Charges"
New York Times, 16 Jul 1981, "Ex-Army Warrant Officer Accused of Being Soviet Spy"
New York Times 24 Sep 1981, "Generals Testify in Espionage Case"

***

1981 - STEPHEN BABA, an ensign in the U.S. Navy, was arrested on 1 October for sending a classified electronic warfare document and two microfilm indices of key code words to the South African Embassy in Washington, D.C. He reportedly asked for an initial payment of $50,000 for the material. Other charges against Baba at the time included armed robbery, extortion, and assault. Baba mailed the documents from his frigate, the USS *Lang*, in September 1981, while stationed at San Diego. The South African Embassy returned the unsolicited materials to U.S. officials. In court testimony it was asserted that Baba had attempted to sell documents to raise money for his fiancee in the Philippines so that she could attend college. He pleaded guilty and was sentenced 20 January 1982 by court-martial to eight years of hard labor.

New York Times, 4 Dec 1981, "Ensign is Accused in Navy Spy Case"
Washington Post, 21 Jan 1982, "Ensign Sentenced to Hard Labor for Sending Data to S. Africa"

***

1982 - OTTO ATTILA GILBERT, Hungarian born U.S. citizen, was arrested 17 April after paying $4,000 for classified documents provided by an Army officer who was working as a U.S. Army double agent under Army control. The officer, CWO Janos Szmolka, had been approached in 1977 by agents of Hungarian military intelligence while on a visit to his mother in Hungary and had reported the contact to Army Intelligence. While stationed in Europe, Szmolka agreed to work as a double agent. In 1981 he received $3,000 for 16 rolls of film of unclassified documents and was offered $100,000 for classified material on weapon and cryptographic systems. Szmolka was reassigned to Fort Gordon, Georgia in 1980, but maintained his contacts with Hungarian intelligence which led to the meeting with Gilbert. Gilbert was convicted of espionage and sentenced to 15 years in prison. This case is considered to be a classic example of recruitment based on a hostage situation since implied threats were made against the Hungarian relations of the U.S. service member.

Washington Post, 20 Apr 1982, "Spying is Charged to New Yorker of Hungarian Origin"
New York Times, 20 Apr 1982, "Native of Hungary is Jailed in South on Spying Charges"

***

1982 - BRIAN E. SLAVENS, Marine Corps PFC, reportedly deserted his sentry post at the Marine's Modified Advanced Undersea Weapons Command, Adak Alaska. He advised his sister that he did not

intend to return to the Marine Corps and that he had visited the Soviet Embassy in Washington, D.C., during late August/early September 1982. Slavens's father alerted the Marine Corps of his son's intent to desert, and abruptly Slavens was arrested by Naval Investigative Service Special Agents on 4 September 1982. During interrogation, Slavens admitted entering the Soviet Embassy in Washington, D.C., and offering to provide information concerning the military installation where he worked in Adak. Slavens denied transferring any classified material to the Soviets, but explained that his intent was to sell U.S. military information for $500 to $1,000. According to Slavens, he was actually inside the Soviet Embassy less than thirty minutes, during which time he was asked to provide an autobiographical sketch and to reconsider his actions. Slavens subsequently requested legal counsel, and his lawyer later agreed for Slavens to undergo a polygraph examination. Slavens was administered a polygraph exam on 5 September 1982, the results of which indicated that he did not disclose any classified information to the Soviets. On 24 November 1982, Slavens pleaded guilty to a charge of attempted espionage at a general court-martial held at Marine Corps Base, Camp Lejeune, North Carolina. He was sentenced to two years confinement and forfeiture of all pay and allowances, and given a dishonorable discharge.

Naval Investigative Service Command, *Espionage*, 1989

***

1982 - BRIAN P. HORTON was a U.S. Navy Intelligence Specialist Second Class, assigned to the Nuclear Strike Planning Branch at the Fleet Intelligence Center, Europe and Atlantic, located in Norfolk, Virginia. Between April and October, 1982, Horton wrote one letter and made four telephone calls to the Soviet Embassy, offering to provide information on the Single Integrated Operations Plan (SIOP). Based upon evidence accumulated during the investigation, Horton chose to plead guilty under a pretrial agreement which included a post-trial grant of immunity. This allowed the Naval Investigative Service to question Horton after his conviction and sentencing for a period of up to six months to determine any damage to national security caused by his actions. (This technique of post-trial grant-of-immunity encourages the suspect to cooperate in an effort to reduce his sentence.) He was sentenced by a general court-martial on 12 January 1983 to six years confinement at hard labor, forfeiture of all pay and allowances, a dishonorable discharge, and reduction in pay grade to E-1 for failing to report contacts with the Soviet Embassy in Washington, D.C., and for attempting to sell classified information to the USSR. No classified information was actually exchanged and no money was received by Horton. His defense attorney argued that Horton was working on a novel and approached the Soviets to learn their *modus operandi*. The prosecution stated that he had attempted to get between $1,000 and $3,000 for classified information.

Washington Post, 14 Jan 1983, “Sailor Sentenced after Bid to Sell Plans to Soviets”
Naval Investigative Service Command, *Espionage*, 1989

***

1983 - WALDO H. DUBBERSTEIN, retired DIA employee and associate of convicted arms smuggler Edwin P. Wilson, was indicted on 28 April on charges of selling U.S. military secrets to Libya. The following day Dubberstein was found dead; his death was later ruled a suicide. Had he been convicted of espionage and of other charges against him, including conspiracy and bribery, Dubberstein would have faced a possible sentence of 57 years and $80,000 in fines. Dubberstein had apparently begun his cooperation with Libya as an outgrowth of his meetings with Edwin P. Wilson who acted as a middleman for passage of information to Libya and receipt of payments to Dubberstein.

Washington Post, 8 May 1983, “The Last Battle of an Old War Horse”
Time, 9 May 1983, “Beyond Justice; an Accused Spy is Dead”

***

1983 - YURIY P. LEONOV, a lieutenant colonel in Soviet military intelligence (GRU), fronting as a Soviet air force attaché, was apprehended on 18 August after receiving 60 pounds of government documents from an editor working under FBI control. The following day Leonov, who had diplomatic immunity, was declared *persona non grata* and expelled from the country. This ended a two year recruitment attempt by Leonov against Armand B. Weiss, an editor of technical publications and former government consultant. Weiss had previously held a Top Secret clearance. In all, Leonov paid Weiss $1,800 for sensitive but unclassified publications on weapon systems. Ultimately, Leonov demanded a classified document. Under FBI direction Weiss provided the item with a large number of highly technical publications for $500 cash. Leonov was arrested by agents waiting outside the office.

Washington Post, 16 Sep 1983, "Soviet Military Spy Caught in FBI Trap"

***

1983 - HANS PALMER WOLD was an Intelligence Specialist Third Class assigned to the USS *Ranger* when he asked for and was given leave from 13 June through 2 July 1983. The leave was granted with the understanding that Wold would stay in the local San Diego area, but around 2 July Wold's command received a message from the American Red Cross, Subic Bay, Philippines, in which Wold requested an extension of leave. Wold's request was granted for five additional days of leave. But he failed to report for duty on 7 July and was listed as an unauthorized absentee. Wold's command then asked the Naval Investigative Service to locate him and turn him over to U.S. Naval Forces in the Philippines at Subic Bay for appropriate debriefing. On 19 July Wold was picked up by NIS Special Agents at his fiancee's residence in Olongapo City, in the Philippines, for being absent without leave. During Wold's apprehension, an undeveloped roll of film was seized. During his debriefing Wold told an intelligence specialist that the roll of film had photographs from a Top Secret publication. Wold admitted he had covertly photographed the publication, "Navy Application of National Reconnaissance Systems (U)" while onboard the USS *Ranger* during June, 1983, and intended to contact the Soviets. On 5 October 1983, Wold pleaded guilty at a general court-martial to unauthorized absence, using marijuana onboard the USS *Ranger*, false swearing, and "making photographs with intent or reason to believe information was to be used to the injury of the U.S. or the advantage of a foreign nation." Wold was sentenced to four years at hard labor; a dishonorable discharge; forfeiture of all pay and allowances; and reduction in rate to E-1.

Naval Investigative Service Command, *Espionage*, 1989

***

1983 - JOHN RAYMOND MAYNARD, Navy Seaman, while on unauthorized absence, was found to have 51 Top Secret documents in his personal locker. Until the time of his arrest in August, Maynard was assigned to the staff of the Commander in Chief Pacific Fleet in Hawaii as an intelligence specialist. He was convicted at a general court-martial for wrongfully removing classified material and was sentenced to ten years confinement.

***

1983 - ROBERT WADE ELLIS, Navy Petty Officer, stationed at the Naval Air Station, Moffett Field, California, reportedly contacted the Soviet Consulate in San Francisco, with an offer to sell classified documents for $2,000. Ellis was arrested in February while attempting to sell documents to an undercover FBI agent. He was convicted at a general court-martial for unauthorized disclosure of classified information and was sentenced to three years confinement.

***

1983 - JAMES DURWARD HARPER, a Silicon Valley free-lance engineer was arrested 15 October for selling large quantities of classified documents to Polish intelligence for a reported sum of $250,000. Harper, who did not hold a clearance, acquired classified material through his wife, **RUBY SCHULER**. Schuler was employed by Systems Control, Inc. of Palo Alto, a Defense contractor engaged in research on ballistic missiles. Between July 1979 and November 1981, Harper conducted a total of a dozen meetings with Polish agents in Europe and Mexico at which times he turned over documents related to the Minuteman ICBM and ballistic missile research. In September 1981 Harper attempted to bargain for immunity from prosecution by anonymously contacting the CIA through a lawyer. Schuler died in June 1983 of complications related to alcoholism. Harper, who eventually pleaded guilty to six counts of espionage, received a life sentence on 14 May.

DoD Security Institute, *Security Awareness Bulletin*, August 1984, Number 4-84
Time Magazine, 31 Oct 1983, "For Love of Money and Adventure"
Washington Post, 18 Oct 1983, "KGB Intelligence 'Windfall'"

***

1983 - ALFRED ZEHE, an East German physicist and operative for East German intelligence was arrested on 3 November 1983—the result of a successful sting operation. On 21 December 1981, Bill Tanner, a civilian engineer employed at the Naval Electronic Systems Engineering Center in Charleston, S.C., walked into the East German Embassy in Washington, D.C., and offered to exchange classified information for money. Tanner was actually a double agent working under the control of the Naval Investigative Service and FBI. The FBI's target was the East German intelligence service, the Ministerium fuer Staatssicherheit (MfS): how it worked and what type of information it was looking for. Zehe was Tanner's primary contact. Zehe is reported to be the first East German operative apprehended in this country. In July 1984, Zehe was freed on $500,000 bail to await trial. He subsequently pleaded guilty and was sentenced on 4 April to 8 years imprisonment with a fine of $5,000. In June 1985, Zehe was traded with three other Eastern Bloc agents for 25 persons who had "been helpful" to the United States.

New York Times, 4 Nov 1983, "East German Held in Espionage Case"
5 Nov 1983, "East German is Denied Bail"
Naval Investigative Service Command, *Espionage*, 1989

***

1983 - PENYU B. KOSTADINOV, a commercial counselor at the Bulgarian Commercial Office in New York was arrested in December at a New York restaurant as he exchanged a sum of money for classified material. Kostadinov had attempted to recruit a graduate student who had access to documents related to nuclear energy. The unnamed American agreed to work under FBI control to apprehend the agent. One of Kostadinov's official functions was to arrange for exchange students between Bulgaria and the U.S. Although Kostadinov claimed diplomatic immunity at the time of his arrest, this was later denied by a Federal court. In June 1985, Kostadinov was "swapped" along with three other Soviet Bloc agents for 25 persons who had "been helpful" to the United States.

Washington Post, 25 Sep 1983, "Bulgarian Man Arraigned"
New York Times, 24 Sep 1983, "Bulgarian Charged as Spy"

***

1983 - JEFFERY LORING PICKERING On 7 June 1983, an individual using the name Christopher Eric Loring entered the Naval Regional Medical Center, Seattle, Washington, acting very erratic and stating that he possessed a large quantity of "secret documents vital to the security of our country." The

individual was in possession of one plastic addressograph card imprinted with the address of the Soviet Embassy, Washington, D.C. During permissive searches of his car and residence by Naval Investigative Service agents, four Government marked envelopes containing classified microfiche and 147 microfiche cards containing a variety of classified defense publications were located. Through investigation, the individual was identified as Jeffery Loring Pickering, who had previously served in the U.S. Marine Corps. During his Marine enlistment, he was described as a thief, thrill seeker, and a perpetual liar. Pickering left the Marines in August 1973, but became dissatisfied with civilian life and began efforts to re-enlist in the military. Pickering assumed an alias, Christopher Eric Loring, hid the facts of his prior USMC affiliation, and enlisted in the U.S. Navy on 23 January 1979. During interrogation, Pickering admitted stealing the classified material from the ship's office of the USS *Fanning* between July and October 1982. Pickering likewise expressed an interest in the KGB, and said he fantasized about espionage. He ultimately admitted mailing a five-page Secret document to the Soviet Embassy, Washington, D.C., along with a typed letter offering additional classified material to the Soviet Union. On 3 October 1983, Pickering pleaded guilty at a general court-martial to several violations including espionage. Pickering was convicted and sentenced to five years at hard labor, forfeiture of $400 per month for 60 months, reduction to E-1, and a bad conduct discharge.

Naval Investigative Service Command, *Espionage*, 1989

***

1984 - ARNE TREHOLT, head of the press section of the Norwegian Foreign Ministry was arrested 20 January by Norwegian authorities while boarding a plane for Vienna. He reportedly had a suitcase of classified documents in his possession. A search of his residence uncovered a collection of 6,000 pages of classified material. Treholt, charged with supplying Secret NATO documents to the KGB, had come under suspicion as early as 1980 while he was serving as a member of the Norwegian delegation to the U.N. in New York. At that time he was placed under surveillance by the FBI. Pre-trial statements and testimony reveal that he received over $7,000 from Soviet agents and that he had been subject to blackmail. It is also believed that Treholt was motivated by pro-Soviet ideological beliefs. Treholt pleaded innocent to charges and underwent an 11-week trial by jury. On 20 June 1985 the Norwegian court found Treholt guilty of seven counts of espionage. He was sentenced to 20 years imprisonment.

New York Times, 29 Jan 1984, “Portrait of Spy as Golden Young Man”
Newsweek, 6 Feb 1984, “The Spy Who Wore Jogging Shoes”

***

1984 - ERNST FORBRICH, a West German automobile mechanic was arrested 19 March in Clearwater Beach, Florida, after paying $550 for a classified military document supplied by an undercover agent posing as an Army intelligence officer. Forbrich was described as a conduit who passed U.S. military secrets to East German Intelligence and by his own admission had been selling documents to East German intelligence for a period of 17 years. Forbrich traveled frequently to the United States, contacting former U.S. military personnel who had served in West Germany. Convicted in June on two counts of espionage, Forbrich was sentenced to 15 years.

Washington Post, 21 Mar 1984, “West German Accused of Spying for East”
New York Times, 21 Mar 1984, “German is Arrested on Spying Charge”

***

1984 - ALICE MICHELSON, an East German national, was apprehended 1 October as she was boarding a flight in New York to Czechoslovakia with tape recordings hidden in a cigarette pack. Michelson, apparently acting as courier for Soviet Intelligence, had been given the classified material by

a U.S. Army sergeant who was posing as a KGB collaborator. Michelson was indicted and held without bail; however, before coming to trial she was "swapped" (June 1985) along with three other Soviet Bloc agents for 25 persons who had "been helpful" to the United States. The FBI has described the case as a classic spy operation.

Washington Post, 3 Oct 1984, "East German Woman Charged with Spying" and
"FBI Agent, German, Analyst in Intelligence Cases"
New York Times, 11 Oct 1984, "East German Indicted in Spy Plot"

***

1984 - RICHARD CRAIG SMITH, Former Army counterintelligence agent, was arrested on 4 April and indicted for selling information to Soviet agents regarding the identities of six double-agents in the U.S. Having failed in business after leaving government service and faced with severe financial difficulties, Smith reportedly met on three occasions with KGB officers in Tokyo and received $11,000 for classified information. Smith himself initiated contact with the FBI in the summer of 1983, claiming he had "conned" the Soviets out of $11,000. Later, Smith claimed that he had been working under the direction of CIA operatives in Honolulu. After months of pre-trial litigation over the admissibility of evidence, Smith was acquitted by a Federal jury on 11 April 1986.

Washington Post, 9 Apr 1984, "Unlikely Character for a Spy Story"
11 Apr 1984, "Spy-Case Suspect....."
13 Apr 1986, "Smith Celebrates His Freedom"

***

1984 - RICHARD MILLER, first member of the FBI to be indicted for espionage was arrested with two accomplices, **SVETLANA** and **NIKOLAI OGORODNIKOV** on 3 October. According to news reports, Miller provided classified documents to the Ogorodnikovs, two pro-Soviet Russian émigrés, and demanded $50,000 in gold and $15,000 cash in return. Miller, who was faced with financial difficulties, is alleged to have been sexually involved with Svetlana Ogorodnikov and was preparing to travel with her to Vienna at the time of his arrest. A search of Miller's residence uncovered several classified documents. At the time of their trial the Ogorodnikovs were accused of having been "utility agents" for the KGB since 1980. After a ten-week trial, and in an agreement with federal prosecutors, each pleaded guilty to one count of conspiracy. Nikolai Ogorodnikov was immediately sentenced to 8 years imprisonment. His wife later received a sentence of 18 years. Richard Miller pleaded innocent and after eleven weeks of testimony, a mistrial was declared. Following a second trial which ended on 19 June 1986, Miller was found guilty of espionage and bribery. His claim that he was trying to infiltrate the KGB as a double agent was rejected by the jury. On 14 July 1986, Richard Miller was sentenced to two consecutive life terms and 50 years on other charges. This conviction following his second trial was overturned in 1989 on the grounds that U.S. District Judge David Kenyon erred in admitting polygraph evidence. He was granted bail in October 1989 while awaiting a new trial on charges that he passed top secret FBI data to the Soviet woman who was his lover. Miller was forbidden to leave the Los Angeles area without special permission and underwent therapy as ordered by the Probation Department. On October 9, 1990, he was convicted on all counts of espionage for the second time, and on 4 February 1991, was sentenced to 20 years in Federal prison. On 28 January 1993, a federal appeals court upheld his conviction. On 6 May 1994, Richard was released from prison following the reduction of his sentence to 13 years by a Federal judge.

Time Magazine, 15 Oct 1984, "Spy vs. Spy Saga"
Washington Post, 4 Oct 1984, "FBI Agent Charged in Espionage"
5 Oct 1984, "Accused Spies Portrayed as Incompetents"

Los Angeles Times, 5 Feb 1991, "Miller Gets 20-Year Term For Spying"

***

1984 - BRUCE LELAND KEARN, Navy operations specialist, assigned as command Secret control officer on board the USS *Tuscaloosa*, was arrested in March 1984 and convicted at a general court-martial for dereliction of duty, and willfully delivering, transmitting or communicating classified documents to unauthorized persons. No nation was named as having received any of the classified materials. While absent without leave, Kearn left behind a briefcase which was found to contain 147 classified microfiche (copies of nearly 15,000 pages of Secret documents), seven Confidential crypto publications, and child pornographic photographs and literature. He was sentenced to four years confinement.

***

1984 - ROBERT E. CORDREY, a Marine private, was convicted 13 August by court-martial of 18 counts of attempting to contact representatives of communist countries for the purpose of selling classified information about nuclear, biological and chemical warfare. Cordrey had been an instructor at the Nuclear, Biological and Chemical Defense School at Camp Lejeune, North Carolina. The charges were not contested and the case was not disclosed to the public until January 1985 due to the extremely sensitive nature of the investigation. Apparently Cordrey attempted to contact Soviet, Czech, East German, and Polish agents. He was sentenced to 12 years at hard labor by the military court; however, his pre-trial agreement with prosecutors limited his jail term to two years.

New York Times, 10 Jan 1985, "Marine Gets 12 Years At Spy Court-Martial"

***

1984 - SAMUEL L. MORISON, civilian analyst with the Office of Naval Intelligence, was arrested 1 October for supplying Jane's Publications with classified photography showing a Soviet nuclear powered carrier under construction. The photographs were subsequently published in *Jane's Defence Weekly* (July 1984). Morison, described as a heavy spender and unhappy with his Navy Department job, had been employed by Jane's as a part-time contributor. A search of his apartment turned up two portions of Navy documents marked Secret. On 17 October 1985, after a seven-day trial, Morison became the first individual convicted under the 1917 Espionage Code for unauthorized disclosure to the press. Also convicted of theft of government property, Morison was sentenced to two years imprisonment on 4 December 1985. The decision was appealed and in April 1988 the conviction was upheld by the 4th U.S. Circuit Court of Appeals. In October 1988 the Supreme Court declined to hear the case, thus endorsing the use of the espionage code for prosecuting cases of unauthorized disclosure.

Washington Post, 3 Oct 1984, "Navy Analyst Arrested in Photo Sale"
29 Oct 1984, "Unlikely Espionage Suspect"
18 Oct 1985, "Morison Guilty of Spying, Stealing Documents"
New York Times, 8 Oct 1984, "Disclosing Secrets to the Press..."

***

1984 - FRANCISCO DE ASSIS MIRA, Air Force computer specialist stationed in Germany, was charged in April with providing classified defense information to East Germany. Mira, a naturalized American born in Spain, and two West German accomplices sold information on American codes and radar to the East German State Security Service. In August 1982, while assigned to duties at a U.S. air base at Birkenfeld, West Germany, Mira photographed the cover and random pages of code books and maintenance schedules of air defense radar installations. He processed the photos, with the help of his girlfriend, and asked two local minor drug dealers to carry the material to East Germany and attempt to

make contact with the KGB. They made several trips between September 1982 and March 1983, each time passing information provided by Mira, and were paid between $1,136 and $1,515 per visit. Realizing he was "in over his head" and feeling used by his accomplices, Mira sought to extricate himself from a bad situation. In March 1983, Mira went to the AFOSI and related what he had done, not realizing how thorough the investigative process would be. Under questioning, Mira claimed that he wanted to become a double agent and that he "wanted to show the Air Force I could do more with my intelligence." But in subsequent interviews he admitted he had originated the idea to commit espionage to make some money, and enlisted the two West Germans to assist him. He was disgruntled because he had not gotten the assignment he had wanted. In August 1984 Mira was dishonorably discharged and sentenced to 10 years confinement. Under a plea bargain he served only seven years of the sentence.

Stars and Stripes, 29 Aug 1984, "Airman is Sentenced for Spy Activities"

***

1984 - KARL F. KOECHER, former CIA employee and his wife, naturalized U.S. citizens of Czech origin, were arrested 27 November as they were preparing to fly to Switzerland. At the time, he was believed to be the first foreign agent to have penetrated the CIA having operated successfully as an "illegal" for Czech intelligence for 19 years. In 1962 Koecher was trained as a foreign agent by Czech intelligence. He and his wife staged a phony defection to the U.S. in 1965 and soon became known as an outspoken anti-Communist member of the academic community in New York City. Both became naturalized citizens in 1971 and Koecher obtained a translator job with the CIA two years later where he translated Top Secret materials until 1975. Koecher, who claimed that he was a double-agent, was arrested after being observed making frequent contact with KGB operatives. According to Federal prosecutors, Mrs. Koecher operated as a paid courier for Czech intelligence until 1983. An FBI agent testified that from February 1973 to August 1983, Karl Koecher passed on to Czech agents highly classified materials including names of CIA personnel. However the case never came to trial. On 11 February 1985, Koecher was exchanged in Berlin for Soviet dissident Anatoly Shcharansky.

New York Times, 28 Nov 1984, "Man Charged with Passing State Secrets"
5 Dec 1984, "Wife is Held in Contempt of Court for Refusing to Testify "
13 Jan 1985, "Intrigue and Countercharges Mark Case of Purported Spies"
Washington Post, 17 Apr 1988, "Moscow Mole in the CIA"

***

1984 - THOMAS PATRICK CAVANAGH, an engineering specialist for Northrop Corporation holding a Secret clearance, was arrested on 18 December and charged with attempting to sell classified documents on Stealth aircraft technology to the Soviets. It is reported that Cavanagh's attempts to contact the Soviet consulate were intercepted. A meeting was proposed at a Los Angeles motel by FBI undercover agents posing as USSR representatives where a deal could be negotiated. During a subsequent meeting, agents provided $25,000 demanded for classified documents and made the arrest. Cavanagh, recently separated from his wife, faced mounting financial difficulties and feared that he was being denied a Top Secret clearance because of indebtedness. It is reported that no serious compromise occurred. Cavanagh pleaded guilty to two counts of espionage and on 23 May 1985 was sentenced to two concurrent life terms in prison.

New York Times, 19 Dec 1984, "Engineer is Held in Scheme to Sell Secrets"
Washington Post, 22 Dec 1984, "Engineer in Secrets Case is Held Without Bail"
DoD Security Institute, *Security Awareness Bulletin*, Dec 1985, Number 1-86

***

1984 - JAY CLYDE WOLFF, 24-year-old auto painter and former Navy enlisted man, was arrested on 17 December in Gallup, New Mexico, for offering to sell classified documents dealing with U.S. weapons systems aboard a U.S. Navy vessel. Wolff who was discharged from the Navy in 1983 met with an undercover agent and offered to sell classified material for $5,000 to $6,000. According to the FBI, a tip led to the meeting with Wolff at a convenience store where he was apprehended. Wolff pleaded guilty to one count of attempting to sell classified documents and on 28 June 1985 the former service member was sentenced to five years in prison.

***

1985 - JOHN ANTHONY WALKER and his son, **MICHAEL LANCE WALKER**, were indicted 28 May by a Federal grand jury in Baltimore on six counts of espionage. The elder Walker, a retired Navy warrant officer who had held a Top Secret Crypto clearance, was charged with having sold classified material to Soviet agents for the past 18 years. During his military career, Walker made some investments in which he lost money. To make up for his losses, in late 1968 at the age of 30, Walker went to the Soviet Embassy in Washington, D.C., and offered his services for purposes of espionage. He compromised key cards used for enciphering messages and also provided information on the encryption devices themselves. At least a million classified messages of the military services and U.S. intelligence agencies were compromised. A Soviet defector said the KGB considered this the most important operation in its history. Michael Walker, a petty officer assigned to the USS *Nimitz*, was accused of providing classified Navy documents to his father for sale to the Soviets. Fifteen pounds of classified material were in his possession at the time of arrest on the *Nimitz*. John Walker's arrest resulted from a tip to the FBI from his former wife. He was apprehended at a Maryland motel after depositing a number of documents at a roadside drop. Soviet embassy official, Alexei Tkachenko, who was spotted in the area, returned to Moscow within days of Walker's arrest. It is also alleged that John Walker recruited his brother, Arthur James Walker and former Navy friend, Jerry Alfred Whitworth as sources of classified information for Soviet intelligence. (see summaries which follow). On 28 October, both John and Michael Walker pleaded guilty to espionage charges under a plea agreement by which the senior Walker agreed to testify in the trial of Jerry Whitworth and to provide full information on what was given to the Soviets in exchange for a lesser sentence for his son. On 6 November 1986, John Walker was sentenced to two life terms plus ten years to be served concurrently. Michael was sentenced to 25 years. A federal grand jury has been convened to pursue some of the unresolved questions including the location of up to $1 million possibly hidden by John Walker, and the involvement of minor players in the espionage ring.

New York Times, 21 May 1985, “Ex-Navy Officer Is Charged With Espionage”
Washington Post, 22 May 1985, “Spy Suspect's Son Queried”
16 Aug 1985, “Lawyers Admit Walker Left Bag”
29 Oct 1985, “2 Walkers Plead Guilty to Spying”
7 Nov 1986, “Walker Gets Life Term; Judge to Oppose Parole”
Naval Investigative Service Command, *Espionage*, 1989

***

1985 - ARTHUR JAMES WALKER, retired Navy Lt. Cmdr., was arrested on 29 May for providing classified material to his brother in 1981 and 1982. Arthur Walker was employed with a Defense contractor in Chesapeake, Virginia, where he reportedly sought work in early 1980 at the urging of his brother, John A. Walker, to gain access to classified documents. During the period of his employment, Arthur Walker provided his brother with several Confidential documents which related to ship construction and design. These were photocopied and returned to the firm's classified container. In all Arthur Walker received $12,000 for his collaboration, much of which he returned to his brother to repay a debt. On 9 August, he was found guilty of seven counts of espionage by a U.S. District Court judge. On 12 November, Arthur Walker was sentenced to life imprisonment and fined $250,000. At the time of

sentencing it was revealed that polygraph tests indicated Walker may have been involved in espionage while on active duty with the Navy.

Washington Post, 7 Aug 1985, "Two Portraits of Arthur Walker: Subversive Plotter"
10 Aug 1985, "Walker Guilty of Espionage On 7 Counts"
Time, 19 Aug 1985, "A Spy Ring Goes to Court"
New York Times, 13 Nov 1985, "Arthur Walker Sentenced to Life; Wider Spying Role

***

1985 - JERRY ALFRED WHITWORTH, collaborator with John A. Walker, surrendered to FBI agents on 3 June following the issue of a complaint charging him with conspiracy to commit espionage. Whitworth, a retired Naval communications specialist who had held a Top Secret clearance, is alleged to have received $332,000 through Walker for highly classified information related to naval communications between 1975 and 1982. FBI sources state that Whitworth had attempted to arrange a meeting with them in 1984 in order to bargain for immunity from prosecution. According to one news item, of all the alleged participants in the "Walker Spy Ring" the damage attributed to Whitworth is thought to be the worst since he is reported to have provided the Soviets with "key lists," which would have enabled them to decode U.S. Naval communications, and classified information about the design of cryptographic equipment. Whitworth pleaded innocent to a 13-count indictment, but during his subsequent trial, defense lawyers admitted that he had passed classified materials to John Walker. However, the argument that he did not know these highly classified cryptographic materials were ending up in Soviet hands was not accepted by the Federal jury. Following a highly publicized three-month trial, Whitworth was convicted on 12 counts of espionage and tax evasion. The former communications specialist received a sentence of 365 years and a fine of $410,000 on 28 August 1986.

Washington Post, 4 Jun 1985, "4th Arrested in Spy Case"
Washington Post, 8 Jun 1985, "Agent Believes Sailor Said He Passed Data"
Washington Post, 14 Jun 1985, "Accused Spy 'A Quiet Man'"

***

1985 - SHARON M. SCRANAGE, operations support assistant for the CIA stationed in Ghana and her Ghanaian boyfriend, **MICHAEL SOUSSOUDIS**, were charged on 11 July with turning over classified information including the identities of CIA agents and informants to Ghanaian intelligence officials. It is reported that a routine polygraph test given to Scranage on her return to the U.S. aroused CIA suspicions. Following an internal investigation, Scranage agreed to cooperate with the FBI in order to arrest Soussoudis, a business consultant and permanent resident of the United States. According to one report, damaging information on CIA intelligence collection activities is likely to have been passed on by pro-Marxist Kojo Tsikata, head of Ghanaian intelligence, to Cuba, Libya, East Germany and other Soviet Bloc nations. Indicted on 18 counts of providing classified information to a foreign country, Scranage subsequently pleaded guilty to one count under the espionage code and 2 counts of violating the Intelligence Identities Protection Act. Fifteen remaining charges were dropped. On 26 November Scranage was sentenced to five years in prison. (This was later reduced to two years.) At the same time Soussoudis who had been charged with eight counts of espionage pleaded *nolo contendere* and was sentenced to 20 years. His sentence was suspended on the condition that he leave the United States within 24 hours.

Washington Post, 12 Jul 1985, "CIA Aide, Ghanaian Face Spy Counts"
14 Jul 1985, "Routine Polygraph Opened Ghanaian Espionage Probe"
20 Jul 1985, "FBI Says Spying Occurred After CIA Order on Ghanaian"

***

1985 - MICHAEL TOBIAS, Navy Petty Officer 3rd Class, along with his nephew, **FRANCIS X. PIZZO** were arrested on 13 August and charged with stealing Top Secret cryptographic key cards from the USS *Peoria*, berthed at San Diego. The pair were also accused of attempting to sell the material to representatives of the Soviet Union for $100,000: Tobias and Pizzo drove to the Soviet Consulate in San Francisco, but arrived during the early morning before regular business hours. Having failed in their initial attempt to contact a "foreign power," and obviously having second thoughts about committing espionage, the pair drove back to San Diego and called the U.S. Secret Service offering to sell the cards back to the Government for amnesty and money by claiming that they were prepared to sell the key material to the Soviets. Several calls were placed to the Secret Service by Pizzo, one of which was traced by the FBI. Also arrested in connection with the case were Tobias's brother, **BRUCE TOBIAS,** and **DALE IRENE** of San Diego. According to government prosecutors, Tobias took the classified cards from the ship instead of shredding them, as was his assignment. Pizzo pleaded guilty to five federal charges and on 7 October was sentenced to 10 years in prison. Bruce Tobias and Dale Irene pleaded guilty to two counts of receiving stolen property. During the four-day trial of Michael Tobias, an NSA official testified that the cards would have provided sensitive information about the location and movement of U.S. and foreign vessels. Two of the 12 pilfered cards have not been recovered. On 14 August Michael Tobias was found guilty of four counts of conspiracy and three counts of theft of government property. The U.S. Attorney stated that Tobias had attempted to leave the country and that he and Pizzo had been seen near the Soviet consulate in San Francisco before their arrests. On 12 November Tobias was sentenced to 20 years imprisonment.

New York Times, 15 Aug 1985, "Sailor is Guilty of Conspiring to Sell Secret Data from Ship"
13 Nov 1985, "Sailor Sentenced to 20 Years for Trying to Sell 11 Navy Codes"
Naval Investigative Service Command, *Espionage*, 1989

** *

1985 - EDWARD L. HOWARD, former CIA agent, was reportedly forced to resign in June 1983 after failing a polygraph examination which indicated his involvement in petty theft and drug use. According to news reports, Howard was one of two former CIA employees (identified by Soviet defector Vitaly Yurchenko) who sold classified information to the KGB. Although placed under surveillance by the FBI at his Albuquerque home, Howard (who had been trained in surveillance and evasion tactics) eluded spotters and fled the country. Howard allegedly met with Soviet agents in Austria in September 1984 and received payment for classified information. He is reported to have revealed to the KGB the identity of a valuable U.S. intelligence source in Moscow, now presumed dead or under sentence of execution. It is also reported that five American diplomats have been expelled from the Soviet Union as *persona non grata* as a result of information provided by Howard. On 7 August 1986, the Soviet news agency TASS announced that Howard had been granted political asylum in the U.S.S.R.

Washington Post, 3 Oct 1985, "2 Ex-CIA Agents Sought by FBI as Possible Spies"
5 Oct 1985, "Affidavit Says Ex-CIA Agent Met High-Level KGB Officers"
20 May 1986, "The CIA Agent who Sold Out"
18 Jul 1986, "5 American Diplomats Caught by KGB"
Newsweek, 23 May 1988, "The Spy Who Got Away"

***

1985 - LARRY WU-TAI CHIN, retired CIA employee, was arrested 22 November and accused of having carried out a 33-year career of espionage on behalf of the Peoples Republic of China. According to media reports, Chin, who retired at 1981 at 63, had been an intelligence officer in the CIA's Foreign Broadcast Information Service. During his career, he held a Top Secret clearance and had access to a wide range of intelligence information. Born in Peking, Chin was recruited by communist intelligence

agents while a college student in the early 1940s. Later he became a naturalized U.S. citizen, worked for the U.S. Army Liaison Office in China in 1943, and joined the CIA in 1952. It is believed that he provided the PRC with many of the CIA's Top Secret Reports on the Far East written over the past 20 years. Chin reportedly smuggled classified documents from his office and between 1976 and 1982, gave photographs of these materials to Chinese couriers at frequent meetings in Toronto, Hong Kong and London. He met with Chinese agents in the Far East as recently as March 1985. Chin may have received as much as one million dollars for his complicity. He was indicted on 17 counts of espionage-related and income tax violations. At his trial which began on 4 February 1986, Chin admitted providing the Chinese with information over a period of 11 years, but for the purpose of reconciliation between China and the United States. On 8 February, Chin was convicted by a Federal jury on all counts. Sentencing had been set for 17 March; however, on 21 February the former CIA employee committed suicide in his cell.

Washington Post, 24 Nov 1985, "Ex-CIA Employee Held as 33-Year China Spy"
New York Times, 30 Nov 1985, "Huge Data Loss from China is Seen from Espionage"
Washington Post, 6 Dec 1985, "Chin Believed Planted in U.S. as Spy"

***

1985 - JONATHAN J. POLLARD, intelligence analyst with the Naval Investigative Service and his wife, **ANNE HENDERSON-POLLARD**, were apprehended on 21 November, outside of the Israeli Embassy in Washington, D.C. as they vainly sought asylum with hope of fleeing the country. Both were charged under the espionage code for selling classified documents to an Israeli intelligence unit for $50,000. It is reported that Pollard's detection resulted from tips from fellow employees that the accused was seeking and copying more classified documents than his job required. Confronted with evidence of his activities by the NIS and the FBI on 15 November, Pollard admitted delivering classified documents to a foreign government agent. He was originally ideologically motivated to pass classified information, but that motivation was later clouded by monetary considerations. At Stanford University in 1976, Pollard is reported to have boasted of working for the Mossad, Israel's foreign intelligence agency. Anne Henderson-Pollard is accused of having intended to sell to representatives of the Peoples Republic of China documents related to the U.S. analysis of China's intelligence operations in this country. Seized at the Pollard residence was a suitcase full of classified materials including many marked Top Secret and related to military capabilities of foreign countries. On 4 June 1986, Pollard and his wife pleaded guilty to espionage and related charges under a plea agreement with Federal officials. Four Israeli nationals were later named as unindicted co-conspirators. On 4 March 1987 Jonathan Pollard was sentenced to life imprisonment. Anne Henderson-Pollard received a five-year term.

New York Times, 28 Nov 1985, "F.B.I. Man Says Naval Analyst Told of Spying"
Washington Post, 4 Dec 1985, "FBI Seeking Pollard Contact Identity"
5 Jun 1986, "Ex-Analyst Pollard Pleads Guilty to Spying"
Naval Investigative Service Command, *Espionage*, 1989

***

1985 - EDWARD OWEN BUCHANAN. In early May 1985, an Air Force Office of Special Investigations (AFOSI) human source provided information that Airman Edward O. Buchanan, in training at Lowry AFB, Colorado, had been phoning the East German Embassy in Washington, D.C. He reportedly wanted to know if Embassy officials had received a letter he had sent in April 1985. According to the source, the letter contained an offer by Buchanan to commit espionage for the East German Government. Unsuccessful at making an East German contact, Buchanan then mailed a letter to the Soviet Embassy in Washington, D.C., fully identifying himself and stating that he had information of a scientific and technological nature that he wanted to sell to the Russian Government. He indicated he would continue to conduct business with the Soviets if they liked his material. At this point AFOSI

agents, posing as Soviet representatives, contacted Buchanan. Believing that he was doing business with Soviet Intelligence Officers, the Airman offered to commit espionage and sell classified documents. He then provided documents to the undercover AFOSI/FBI agents which he claimed were classified Secret and was paid $1,000. Buchanan was apprehended immediately. A later examination of the documents disclosed that they were copies of unclassified articles from an electronics magazine. During an interview following his arrest, Buchanan admitted contacting the East German Embassy and the Soviet Embassy for the purpose of committing espionage. Buchanan also admitted that, although he did not have access to classified information at that time (because of his student status), he planned to sell classified information once his clearance had been granted and he was assigned to a base in Germany. At the time he was being processed for a Top Secret - Special Compartmented Information clearance. His stated intention was to establish a business relationship with the Soviets by selling bogus material to "get my foot in the door" and then later sell classified information. He would then "sell as much classified material as he could until he made enough money to live comfortably." Buchanan was court-martialed on 26 August 1985, and sentenced to 30 months confinement, reduction to Airman Basic, forfeiture of all pay and allowances, and a dishonorable discharge.

***

1985 - RONALD WILLIAM PELTON, former communications specialist with the National Security Agency for 14 years, was identified as a spy for the Soviet Union based on facts provided by defector Vitaly Yurchenko. Arrested in Annapolis on 25 November, Pelton admitted making contacts with the Soviets in 1980, a year after he left NSA. At the time he was faced with serious financial difficulties. Pelton reportedly visited the Soviet Embassy in Washington where he agreed to sell classified information and subsequently made several trips to Vienna Austria where he was debriefed at length by the KGB. During his employment in NSA, Pelton had access to a wide range of highly sensitive information. He allegedly received $35,000 from the Soviets between 1980 and 1983 for information about highly classified U.S. intelligence collection projects targeted at the Soviet Union. Pelton was indicted 20 December on six counts related to espionage. Despite his statement at the time of arrest, Pelton pleaded not guilty. Following a highly publicized trial, Pelton was convicted (5 June 1986) on one count of conspiracy and two counts of espionage. On 6 December 1986, he was sentenced to three concurrent life sentences.

Washington Post, 26 Nov 1985, "FBI Says Spy Suspect Admits Selling Data"
New York Times, 28 Nov 1985, "Ex-Security Agency Employee Said to Have Admitted Spying"
Washington Post, 7 Dec 1985, "Accused Spy Ronald Pelton Was Preoccupied with Money"

***

1985 - RANDY MILES JEFFRIES, messenger for a private stenographic firm in Washington, D.C., was arrested on 14 December and charged with attempting to deliver national defense secrets to the Soviet Union. The firm, a cleared contractor facility, had transcribed closed hearings of the House Armed Services Committee. Jeffries allegedly provided Soviet military officials with at least 40 "sample pages" of Secret and Top Secret transcripts from congressional hearings, offering to hand over a complete package of three documents for $5,000. The investigation of Jeffries began after he was observed by U.S. agents entering the Soviet Military Office in Washington. An FBI undercover agent posing as a Soviet representative contacted the messenger at his residence and arranged a meeting later in the day at a local hotel. Jeffries was arrested as he left the meeting. From 1978 to 1980, he was a support employee for the FBI and reportedly held an agency security clearance. In March 1983 he was convicted of possession of heroin and completed a program for rehabilitation from drug abuse in July 1985. Jeffries entered a plea of guilty on 23 January 1986. On 13 March, Jeffries was sentenced by a Federal judge to from three to nine years imprisonment. As stated by the court at the time of sentencing, it was obvious that poor

security practices at the cleared facility were major contributing factors leading to the loss of classified information.

Washington Post, 22 Dec 1985, "FBI Agent Says Suspected Spy Offered to Sell Him Document"
24 Dec 1985, "Transcripts Tied to Jeffries Had Strategic Data"
DoD Security Institute, *Security Awareness Bulletin* 2-90

***

1986 - BRUCE D. OTT, Airman 1st Class, assigned duties as an administrative clerk at Beale Air Force Base, was arrested 22 January by FBI and Air Force Security agents at a Davis, California, motel as he attempted to sell classified information to undercover agents posing as Soviet representatives. One of the documents cited is "The SAC Tactical Doctrine for SR-71 Crews." At that time, Beale AFB was the home base of SR-71 "blackbird" reconnaissance aircraft. It is reported that Ott tried to contact representatives at the Soviet consulate in San Francisco during the month of January. His communication was intercepted and no classified information actually changed hands. Military prosecutors contended that Ott hoped to be paid up to $160,000 for his information. Following an eight-day court martial proceeding, Ott was found guilty and on 7 August was sentenced to 25 years in prison.

New York Times, 29 Jan 1986, "Airman in California Charged in New Spy Case"
1 Feb 1986, "Details are given on Spying Charge"

***

1986 - ROBERT DEAN HAGUEWOOD, Petty Officer 3rd Class was arrested 4 March by agents of the Naval Investigative Service after allegedly selling part of a Confidential aviation ordinance manual to an undercover police officer. Haguewood, who was stationed at the Pacific Missile Test Center at Point Mugu Naval Air Station near Oxnard, California, reportedly asked around town for someone who would pay for secret information about Naval ordinance. He was placed under surveillance by agents of the Naval Investigative Service who with the FBI and local police officials made the arrest on 4 March after Haguewood receive a payment of $360 for the classified document at a beach location. No contact was made with foreign representatives and no information is known to have been compromised. Haguewood was reported to have had serious financial problems. On 20 June, Haguewood pleaded guilty under a plea-bargain agreement and receive a sentence of two years from a military court.

Washington Post, 20 Jun 1986, "Sale of 'Secrets' To Put Sailor Behind Bars"
New York Times, 11 Mar 1986, "Navy Man Arrested in Spy Case"
Washington Post, 11 Mar 1986, "Sailor Allegedly Tried to Sell Manual"

***

1986 - VLADIMIR M. ISMAYLOV, senior Soviet military attaché was arrested on 19 June at a remote site in Prince George's County, Maryland, after retrieving Secret documents left by a U.S. Air Force officer who was working undercover with counterespionage agents of the AFOSI and the FBI. Until his expulsion for activities incompatible with his diplomatic role, Col. Ismaylov was the highest ranking air force officer at the Soviet Embassy. Ismaylov, apprehended as he buried a milk carton with $41,100 for the U.S. officer, scuffled briefly with FBI agents. According to an FBI spokesman, the Soviet attaché was after information about the Strategic Defense Initiative research program, and data on the cruise missile, stealth bomber, and a hypersonic passenger jet known as the Trans-Atmospheric Vehicle. The operation was run by the GRU (Soviet military intelligence). According to the U.S. officer, the Soviets evaluated the USAF officer for nearly a year before asking him to photograph classified documents. All transactions and communications were to be carried out by the use of "dead drops" at remote locations.

Washington Post, 21 Jun 1986, "Soviet Attaché Arrested, Expelled for Receiving Document"

***

1986 - GENNADIY F. ZAKHAROV, Soviet physicist employed at the United Nations Secretariat was arrested on 23 August on a Queens, New York, subway platform as he gave $1000 to an employee of a U.S. Defense contractor for three classified documents. Zakharov, who did not have diplomatic immunity, had attempted to recruit the employee over a period of three years. At the time of Zakharov's first approach, the individual, a Guyanese national and resident alien of the U.S., was in his junior year at Queens College, New York. Zakharov met with the student on numerous occasions and paid several thousand dollars for a wide range of technical but unclassified information about robotics, computers, and artificial intelligence. At the time of Zakharov's first approach in April 1983, the recruitment target, identified only by the code name "Birg," informed the FBI and agreed to work under FBI control in order to apprehend the Soviet agent. Following his graduation in 1985, Birg obtained a position with a high-technology firm. Under FBI direction, he agreed to sign a ten-year written contract with Zakharov to provide classified information. Money to be paid by the Soviets was to be determined by the quantity and quality of the information. On 30 September, Zakharov pleaded no contest to espionage charges and was ordered to leave the country within 24 hours. Zakharov's expulsion came less than 24 hours after the release of American correspondent Nicholas Daniloff who had been arrested in the Soviet Union for alleged espionage activities.

New York Times, 24 Aug 1986, "A Soviet Official Assigned to U.N. is Seized as a Spy"
25 Aug 1986, "Russian's Arrest Called Example of Spy Threat"
26 Aug 1986, "U.S. Investigating Further Spy Cases in New York Area"

***

1986 - ALLEN JOHN DAVIES, former Air Force sergeant and, at the time of his arrest, a lab technician at a Silicon Valley defense contractor was formally charged on 27 October with trying to pass classified information to the agents of the Soviet Union. Davies, a ten-year veteran who was separated from active service for poor job performance in 1984, had held a Secret clearance during his military service and worked as an avionic sensors system technician. According to the FBI, on 22 September Davies met with an FBI undercover agent posing as a Soviet official in San Francisco's Golden Gate Park. During the meeting Davies provided detailed verbal information and a hand drawing concerning U.S. reconnaissance technology. At a second meeting in October he provided additional classified information. According to Davies's recorded statement, he was motivated "out of revenge because of the unfair way he was treated while in the Air Force." He is also quoted as saying that he wanted to do something to embarrass the United States and to interfere with the effectiveness of its reconnaissance activities. Asked why he waited two years before providing the information, Davies said he waited "just to make sure they couldn't link me with it if I told anybody, just sort of ... hide my trail." Davies, born in Eastleigh, England in 1953, became a naturalized U.S. citizen at the age of eleven. Since October 1984, he had been employed by Ford Aerospace and Communications Corp. in Palo Alto. Federal officials stated that the former airman did not currently hold a clearance and that no information from the contractor facility was involved in the case. Davies was released on $200,000 bail with the condition that he undergo psychological evaluation. But on 27 May 1987 he pleaded guilty to a reduced charge of attempting to communicate secrets to an unauthorized person. Davies was sentenced on 27 August 1987 to five years in prison.

Washington Post, 28 Oct 1986, "FBI Arrests Ex-Airman on Espionage Charges"
Los Angeles Times, 28 Oct 1986, "San Jose Man Angry at AF Is Arrested as Would-Be Spy"

***

1986 - MICHAEL H. ALLEN, a retired Navy Senior Chief Radioman employed at the Cubi Point Naval Air Station in the Philippines, was arrested on suspicion of espionage by Navy security agents on 4 December. Allen, who had been working as a civilian clerk, retired from the Navy in 1972. The employee confessed to passing classified U.S. counterintelligence reports to Philippine intelligence officers after seeing a videotape of himself hiding documents in his pockets. When apprehended he had a photocopy of a Secret page on his person; six other classified documents were seized at his residence. The charges covered the period between July and December 1986 during which time he was accused of photocopying and removing classified material from the communication center. According to the Naval Investigative Service, Allen's activities may have resulted in the compromising of important Filipino intelligence sources. Prosecutors argued that Allen's main reason for providing secrets to the Filipinos was to promote his local business interests which included a used car dealership, a bar, and a cockfighting ring. On 14 August 1987, a court martial in San Diego found Allen guilty of 10 counts of espionage and sentenced him to eight years in prison. The six-officer panel also imposed a $10,000 fine on the former radioman.

New York Times, 12 Dec 1986, "Navy Employee Held in Espionage-Related Case"
*Los Angeles Times***,** 15 Aug 1987, "Linked to Filipinos; Ex-Navy Man Found Guilty

***

1986 - CLAYTON J. LONETREE, Marine Corps security guard at the U.S. Embassy in Moscow from September 1984 to March 1986, and later in Vienna, was placed under detention on 31 December 1986 after he acknowledged his involvement with a female KGB officer, Violette Seina, who had previously been a telephone operator and translator at the U.S. Embassy in Moscow. Soon after their relationship began, Seina introduced Lonetree to her "Uncle Sasha" who was later identified by U.S. intelligence as being a KGB agent. It was alleged at the time that Sgt. Lonetree had a sexual liaison with Seina, and had in fact allowed Soviet agents after-hours access to the U.S. Embassy. In December 1986, Lonetree turned himself in to authorities at the U.S. Embassy in Vienna, Austria, where he was stationed. Also arrested and charged with collaboration with Lonetree was Corporal Arnold Bracy who was also alleged to have been romantically involved with Soviet women. As the investigation proceeded, five other Marine guards were detained on suspicion of espionage, lying to investigators, or for improper fraternization with foreign nationals. Lonetree was tried on 13 counts including espionage. Among these counts were charges that he conspired with Soviet agents to gather names and photographs of American intelligence agents, to provide personality data on American intelligence agents, and to provide information concerning the floor plans of the U.S. Embassies in Moscow and Vienna. On 21 August 1987 Lonetree was convicted of espionage and 12 related counts by a military court. Three days later he was sentenced to 30 years imprisonment, fined $5,000, loss of all pay and allowances, reduced to the rank of private, and given a dishonorable discharge. Espionage charges against Bracy and all of the other Marines have since been dropped. According to reports in late 1987, intensive investigations have led to the conclusion that the former guards did not, as earlier believed, allow Soviet agents to penetrate the U.S. Embassy in Moscow. In May, 1988, Lonetree's sentence was reduced to 25 years, in 1992 to 20 years, and later to 15 years. In February 1996 he was released.

Washington Post, 10 Feb 1987, "'Success Story' Marine May Face Trial for His Life"
30 Jul 1987, "Envoy Blamed for Lax Security"
17 Jan 1988, "Spy Scandal Snowballed, Melted Away"
Naval Investigative Service Command, *Espionage*, 1989
Richmond Times-Dispatch, 25 February 1996, "Lonetree May Find Stigma Lives On"

***

1987 - HOU DESHENG, a military attaché of the Peoples Republic of China was detained by FBI agents on 21 December while attempting to obtain Secret National Security Agency documents from a federal employee. Desheng was taken into custody at a restaurant in Washington's Chinatown after

accepting what he believed to be classified NSA documents. The federal employee, a U.S. citizen, had been working under FBI direction. Arrested at the same time was **ZANG WEICHU,** a PRC consular official in Chicago. Both diplomats were asked to leave the country as a result of "activities incompatible with their diplomatic status" – the first Chinese diplomats expelled since formal relations were established with the PRC in 1979.

New York Times, 31 Dec 1987, "2 Chinese Depart in Espionage Case"
Washington Post, 31 Dec 1987, "U.S. Expels Two Chinese Diplomats as Spies"

***

1987 - MIKHAIL KATKOV, a second secretary assigned to the Soviet Mission at the United Nations was detained in New York City on 17 December as he was attempting to acquire defense related technology. He was ordered to leave the country on the following day. Although few details about the case have been released, officials acknowledged that Katkov had been under surveillance for "some time" and that his activities amounted to "not a huge deal, but nonetheless serious espionage." According to a State Department source, Katkov is the 42nd Soviet representative to have been expelled from the United States for espionage since 1950.

Washington Post, 18 Dec 1987, "Soviet Aide Detained by FBI, To Be Expelled for Espionage"
New York Times, 19 Dec 1987, "U.S. is Expelling Soviet Diplomat at U.N. as a Spy"

***

1988 - DANIEL WALTER RICHARDSON, a U.S. Army sergeant stationed at the Aberdeen Proving Ground, Maryland, was arrested on 7 January and charged with attempting to spy for the Soviet Union. Richardson reportedly intended to offer unspecified national defense information to Soviet representatives in exchange for money. No information is believed to have been compromised. Officials stated that Richardson was apprehended after electronic surveillance picked up his efforts to contact Soviet representatives. This led to his negotiation with an undercover government agent posing as a Soviet. He was arrested at the Holiday Inn in Aberdeen Maryland (with an unclassified military manual and circuitry from the M-1 tank in his possession) as he attempted to meet with the undercover agent. An Army spokesman stated that Richardson had a Secret clearance but "no ready access to classified materials." Although trained as an instructor, his job was to issue tools to students at the Ordinance Center School at Aberdeen. "Money and revenge against the military" have been identified by an administration official as Richardson's chief motivations for espionage. Described as a mediocre soldier, Richardson was demoted in August 1987 for repeated tardiness. He was charged at the time of arrest with espionage, failure to report contacts with a foreign government, theft, and unauthorized disposition of government property. On 26 August 1988 Richardson was sentenced by a military jury to ten years in prison, fined $36,000, and discharged with a bad conduct record.

New York Times, 15 Jan 1988, "Army Sergeant is Arrested on Espionage Charges"
Washington Post, 16 Jan 1988, "Soldier Had No Access to Army Secrets"

***

1988 - WILFREDO GARCIA, Navy Master-at-Arms 1st Class, was found guilty of espionage on 22 January following a two-year investigation by agents of the Naval Investigative Service and the FBI. In late 1985, NIS and FBI officials received information that a civilian businessman in Vallejo, California, was attempting to sell classified Navy documents to representatives of a foreign government. A cooperating witness identified Garcia, who was then stationed at Mare Island Naval Shipyard, as the source. Confidential documents stolen by Garcia dealing with submarine activities were sold to the civilian for $800,000 with a promise of more money when they were resold to a foreign government. Evidence indicated that the final destination could have been an East-Bloc country. The espionage

scheme resulted in a number of classified documents being taken to the Philippines for sale to a foreign power there. Participants in the conspiracy couriered the documents on commercial aircraft and had gathered the material in a residence in Manila. Naval Investigative Service agents in Manila entered the home with a search warrant and recovered the documents before the planned sale. At a general court-martial convened in January 1988, Garcia was found guilty of espionage, conspiracy to commit espionage, larceny, conspiracy to commit larceny, sale of government property, and violations of military regulations. He was sentenced to 12 years confinement, reduced in rank to E-1, forfeited all pay and allowances, and received a dishonorable discharge from the Navy. Garcia had served in the Navy for 15 years.

Naval Investigative Service Command, *Espionage*, 1989

***

1988 - STEPHEN JOSEPH RATKAI was arrested by Canadian authorities on 11 June and charged with attempting to obtain U.S. classified military documents related to the operation of a U.S. Navy installation at Argentia, Newfoundland. Although born in Canada, Ratkai was brought up in Hungary, his father's native country, after the death of his Canadian mother. As an adult he returned to Canada to work as a short-order cook, but made frequent trips back to Hungary. Ratkai was seized as a result of a double agent operation begun two years earlier by the U.S. Naval Investigative Service and Canadian intelligence: On 2 December 1986 Donna Geiger walked on board a Soviet scientific research vessel, the Akademik Boris Petrov, which was temporarily docked in the harbor of St. John's, Newfoundland. Geiger, a Navy lieutenant, was a double agent who had been recruited by the Naval Investigative Service. She was stationed at the U.S. Naval Facility in Argentia, Newfoundland. On board the Soviet ship, she portrayed herself as a "disgruntled female naval officer ... working in a world dominated by men ... assigned to an isolated duty station." She brought classified material to prove her intentions. Two months later she received a letter indicating someone would meet with her. Finally in May 1987, acting on directions she received by mail, she met her contact, "Michael," in the parking lot of the Hotel Newfoundland in St. John's. She was given money and some tasking to collect information. A week later Lt. Geiger met Michael in a restaurant. Classified information was exchanged for money. During this meeting she was tasked to provide information on the highly classified Sound Underwater Surveillance System and the Naval Facility Argentia's area of responsibility. After several more meetings, Michael was identified as Ratkai. At their last meeting in June 1988, Geiger steered Ratkai to a room at the Hotel Newfoundland which was outfitted with surveillance equipment. More money and classified information was exchanged. When Ratkai left the room, he was arrested. No damage is reported to have occurred. On 6 February 1989 Ratkai pleaded guilty to one general charge of spying on behalf of the Soviet Union from May 1987 to June 1988 and one charge of attempted espionage. On 9 March 1989 the Newfoundland Supreme Court sentenced Ratkai to two concurrent nine-year prison terms.

New York Times, 16 Jun 1988, "Canada Holds Suspect in Spying on U.S. Navy"
St. Louis Post-Dispatch, 11 Mar 1989, "Spy Gets 9 Years"
Naval Investigative Service Command, *Espionage*, 1989

***

1988 - GLENN MICHAEL SOUTHER. On 11 July, Soviet newspaper *Izvestia* announced that Souther, a former navy photographic specialist who disappeared in May 1986, had been granted political asylum in the Soviet Union. Just before his disappearance, Souther, a recent graduate with a major in Russian Studies from Old Dominion University, was questioned by FBI counterintelligence agents. According to one source, investigators were acting "on more than suspicions, but didn't catch him in the act of espionage, and thus couldn't hold Souther at the time he was questioned." While attending college, Souther had been assigned as an active reservist to the Navy Intelligence Center in Norfolk where he had

access to classified information. Souther's sudden disappearance was of considerable concern to FBI and Navy officials since the former Navy enlisted man had held special security clearances while on active duty with the Sixth Fleet in the early 1980s. During that time he had access to highly classified photo-intelligence materials. Souther joined the Navy in 1975 and left active duty in 1982 with the position of photographers mate. According to the Soviets, the former Navy specialist had asked for asylum because "he had to hide from the U.S. special services which were pursuing him groundlessly." Described as a bright but undisciplined young man by former teachers and acquaintances, Souther reportedly had wanted to become a U.S. Naval officer, but had been turned down as a Navy officer candidate. On 22 June 1989, at the age of 32, he reportedly committed suicide by asphyxiation after shutting himself in his garage and starting his Russian-made car. Russian newspapers suggested he had been disappointed by aspects of Soviet life after defecting in 1986 and was prone to depression.

Washington Post, 18 Jul 1988, "Ex-Sailor Defects to Soviets"

***

1988 - CLYDE LEE CONRAD, retired Army Sergeant First Class, was arrested on 23 August in West Germany and charged with copying and transmitting classified documents to the Hungarian intelligence service for nearly a decade. He was recruited in 1974 by a Hungarian-born immigrant, **ZOLTAN SZABO**, a veteran of Vietnam who served as an Army Captain in Germany. Szabo began working for Hungarian intelligence in 1967. (He was convicted of espionage by an Austrian court in 1989, but served no jail time because of his cooperation with authorities in the prosecution of Conrad.) Two Hungarian-born doctors arrested at the same time in Sweden are said to have acted as couriers in the espionage operation and Conrad is believed to have hired at least a dozen people in the U.S. Army to supply classified information—one of the biggest spy rings since World War II. Conrad's recruits continued to work for him after returning to the U.S., illegally exporting hundreds of thousands of advanced computer chips to the East Bloc through a phony company in Canada. In June 1990, former Army sergeant **RODERICK JAMES RAMSAY**, 28, was arrested in Tampa, Florida, following a two-year investigation. Ramsay worked in West Germany from 1983 to 1985 directly under Conrad. He provided Conrad with sensitive documents on the use of tactical nuclear weapons by U.S. forces and NATO allies and plans for the defense of Europe, and manuals on military communications technology. Conrad was granted a Top Secret security clearance in 1978 when assigned to the U.S. 8th Infantry Division headquarters in Bad Kreuznach, Germany. Despite his administrative specialist's job which gave him access to extensive classified materials, Conrad had not been subject to a periodic reinvestigation before his retirement in 1985. Documents provided to Hungarian agents concerned NATO's plans for fighting a war against the Warsaw Pact—detailed descriptions of nuclear weapons and plans for movement of troops, tanks and aircraft. Conrad, in charge of a vault where all the 8th Infantry Division's secret documents were kept, took suitcases stuffed with classified papers out of the base. The former sergeant is reported to have received more than $1 million for selling secrets. The two Hungarian couriers, **SANDOR** and **IMRE KERCSIK** were sentenced by a Swedish court on 18 October to 18 months in prison. In 1989 Conrad was charged with treason under West German law. It took more than a year to charge him formally due to the complexity of the case which initially was declared one of espionage and then broadened to include the more serious charge of treason. Tried in a West German court, Conrad was sentenced to life imprisonment on 6 June 1990.

Washington Post,	27 Aug 1988, "U.S. Ex-Sergeant Accused in Spy Case Not Given Mandatory Security Check"
St. Louis Post-Dispatch	2 Sep 1989, "Former U.S. Sergeant Accused of Treason"
Richmond Times-Dispatch,	7 Jun 1990, "Former GI Given Life for Spying"
Los Angeles Times	9 Jun 1990, "Alleged Spy Called Brilliant, Erratic"

***

1988 - DAVID FLEMING, Navy Chief Petty Officer, was convicted by a six-member military court on 4 October for the theft of 16 Secret photographs and four classified training manuals which he had at his home. At the time of his arrest in October 1987, Fleming was chief photographer aboard the submarine La Jolla, based at San Diego, California. At that time Federal agents found classified material in Fleming's apartment. Fleming contended that cramped quarters aboard the ship led him to develop photographs at home. Concluding that he knew that the materials, if kept at home, could result in damage to national security, the court convicted Fleming under statutes which apply to acts of espionage. However, no evidence was presented to the court that the Chief Petty Officer had intended to provide classified materials to representatives of another country. Fleming was sentenced to four years confinement and was given a bad conduct discharge from the Navy. In April 1989 a Navy parole board in San Diego recommended that the remainder of the four-year sentence be commuted. He was released on parole in 1990.

Los Angeles Times, 5 Oct 1988, "Sailor Gets Prison in Classified Data Case"
San Diego Union, 15 Apr 1989, "Early Release Backed for Sailor Convicted on Security Charges

***

1988 - HENRY OTTO SPADE, a former Navy radio operator, was arrested in Mountain Home, Arkansas, on 17 November for the unauthorized possession of two Top Secret documents. One of the documents was a cryptographic key card. Spade, who was discharged from the Navy in April, 1988, stole the items while on active duty, but had reportedly made no attempt to sell them to any person or foreign government. While in the Navy, Spade served aboard the USS *Midway* and the USS *Bristol County*. Charged with one count of espionage, Spade pleaded innocent and was released on $25,000 bond. Spade faced up to 10 years in prison and a $250,000 fine when convicted, but on 14 March 1989 was sentenced to three months probation.

Washington Post, 18 Nov 1988, "Ex-sailor charged in secrets case"

***

1988 - THOMAS JOSEPH DOLCE, civilian research analyst at Aberdeen Proving Ground, Maryland, admitted in Federal court on 11 October that he had supplied scores of Secret documents related to Soviet military equipment to the Republic of South Africa between 1979 and 1983. Dolce, who had been under investigation by the FBI since April, resigned from his position on 30 September "for personal reasons." Dolce had held a Secret clearance at the Army Material Systems Analysis Activity at Aberdeen where he had been employed since 1973. In pleading guilty to a single count of espionage, he acknowledged passing documents on 40 or more occasions by mail or in person to military attachés at the South African Embassy in Washington and at South African missions in London and Los Angeles. According to Dolce, he was motivated by ideological rather than financial reasons and had a long-term interest in the Republic of South Africa. He had in fact moved to South Africa in 1971, but later returned to the U.S. because of better employment opportunities. Prior to 1971 Dolce had been a U.S. Army clandestine warfare specialist. His contacts with South African representatives began when he sent them an unclassified paper on clandestine warfare which he had written. There is no evidence that Dolce received money in exchange for documents. On 20 April 1989, the former analyst was sentenced to 10 years in prison and fined $5,000.

Washington Post, 12 Oct 1988, "Md. Man Admits to Espionage for South Africa"
13 Oct 1988, "Spy for S. Africa Called Reserved

***

1988 - JAMES HALL III, Army Warrant Officer, was arrested on 21 December in Savannah Georgia after bragging to an undercover FBI agent that over a period of six years he had sold Top Secret intelligence data to East Germany and the Soviet Union. At the time, Hall believed that he was speaking to a Soviet contact. During this conversation he claimed that he had been motivated only by money. He told the FBI agent posing as a Soviet intelligence officer, "I wasn't terribly short of money. I just decided I didn't ever want to worry where my next dollar was coming from. I'm not anti-American. I wave the flag as much as anybody else." Also arrested in Belleair, Florida, was **HUSEYIN YILDIRIM** (nicknamed, "the Meister") a Turkish national who served as a conduit between Hall and East German agents. He was working as a civilian mechanic at an Army auto shop in Germany at the time. According to FBI sources, Hall started passing documents to East German agents in 1982 while serving in West Berlin as a communications analyst monitoring Eastern-bloc cable traffic. Later, Hall was transferred to Frankfurt where he continued to pass "massive amounts" of highly classified data on communications intelligence. Hall is believed to have received over $100,000 from agents of two countries during this period of time. In July 1987 he was reassigned to Ft. Stewart, near Savannah, Georgia. Hall had been under investigation by FBI and Army counter-intelligence agents for several months before his arrest and had been observed meeting Yildirim three times in November and December. Hall's detection as an espionage source may have resulted from reports that Hall was living in a style far above what his pay scale would allow. According to U.S. officials, the operation appears to have inflicted serious damage on U.S. electronic intelligence collection activities in Europe. On 9 March 1989 Hall was sentenced to 40 years in prison, fined $50,000 and given a dishonorable discharge. Yildirim was convicted 20 July 1989 of scheming with Hall and sentenced to life. Prosecutors contended that from 1982 to 1988 Yildirim carried classified military intelligence from Hall to East Bloc agents and returned with money.

New York Times, 22 Dec 1988, "Army Technician and a Civilian are Held as Spies for Soviet Bloc
19 Jul 1989, "Jury Hears Tale of Spy Who Did It Out of Greed"
Washington Post, 23 Dec 1988, "Spy Suspect Said to Act Prosperous"
Newsweek, 2 Jan 1989, "Top Secrets for Sale?"

***

1988 - DOUGLAS TSOU, Chinese-born former FBI employee was indicted in 1988 on one count of espionage following his admission that in 1986 he had written a letter to a representative of the government of Taiwan in which he revealed the identity of an intelligence officer of the Peoples Republic of China. According to testimony at the trial (which was delayed until October 1991), the unidentified agent operating in Taiwan had unsuccessfully approached the FBI with an offer to work as a double agent. Although the information Tsou passed to a Taiwanese representative in Houston was classified as SECRET, Tsou claimed that he considered the information to be declassified since the offer was not accepted. Tsou fled to Taiwan when the communists rose to power on the mainland in 1949 and moved to the U.S. twenty years later where he became a naturalized U.S. citizen. He worked for the FBI from 1980 to 1986, first in San Francisco and later in Houston. On 4 October 1991, Tsou was found guilty as charged. However, prosecutors claimed that this represented only "the tip of the iceberg" of what Tsou gave to Taiwanese officials during his six years with the FBI. On 2 January 1992, Tsou was sentenced to a ten-year federal prison term.

Houston Chronicle 22 Jan 1992, "Ex-FBI Translator Sentenced for Passing Secrets to Taiwan"

***

1989 - TOMMASO MORTATI, former U.S. Army paratrooper was arrested in Vincenza by Italian authorities on charges of having passed top-secret documents to Hungarian military intelligence services. According to European news reports, the former Army sergeant who was born in Italy, confessed to disclosing secrets about American and NATO bases in Italy and claimed he belonged to a still-active

espionage network. He is presumed to have been a member of the same network that included the Conrad spy ring in Bad Kreuznach, Germany. Conrad was arrested in August 1988 and has since been sentenced by a German court to life imprisonment. Mortati was born in Italy but later emigrated to the United States where he obtained U.S. citizenship. He left the army in 1987 but remained in Italy as his American wife continued to work for the U.S. Army base in Vincenza. Mortati's arrest followed that of Hungarian-born naturalized American **ZOLTON SZABO** who recruited Mortati in 1981, sent him for two weeks of training in Budapest, and continued to be his contact. Mortati is said to have confessed to Italian authorities that he attempted to bribe several Italian officers in 1984 and 1985, offering money for information. Press reports state that Italy's military secret service was informed about Mortati's activities by German and Austrian counterintelligence authorities. A search of Mortati's home revealed a hidden two-way radio used to transmit his reports in code. Up until the time of his arrest, he had received $500 a month from the Hungarian Intelligence Service plus a payment for every report filed, based on its importance. Mortati was convicted in an Italian court and after a period of incarceration has been released.

This summary is based on European media items and an ABC Television News report.

***

1989 - CRAIG DEE KUNKLE, former Chief Petty Officer who specialized in anti-submarine warfare was arrested on 10 January as he attempted to sell classified information for $5,000 to FBI agents posing as Soviet diplomats. The arrest took place at a Williamsburg, Virginia, motel. On 9 December Kunkle mailed a packet of diagrams, photographs and information related to anti-submarine warfare tactics to an Alexandria, Virginia, post office box he believed to be a Soviet drop point. The material was collected by Federal agents who had been in communication with Kunkle on six previous occasions. An investigation by the Naval Investigative Service and FBI began in early December 1988 when Kunkle's attempt to contact the Soviet Embassy in Washington was intercepted. Kunkle had served for 12 years in the Navy in anti-submarine squadrons in the Atlantic and Pacific fleets and was discharged in 1985 under less than honorable conditions – reportedly for multiple incidents including indecent exposure. Kunkle also had a history of alcohol and drug abuse in addition to marital and financial problems. During his period of active duty, he held a Secret clearance. The former Chief Petty Officer had since been employed as a security guard at a local hospital. At the time of arrest Kunkle stated that he offered to sell classified information because he was short of cash and angry with the Navy. Kunkle was indicted on one count of attempted espionage and ordered held without bond. He pleaded not guilty to the charge. On 4 May 1989 Kunkle changed his plea to guilty because, he said, he did not want to subject his family to a trial. He had faced a maximum sentence of life in prison and a $250,000 fine. The judge imposed a 12-year sentence (agreed upon by prosecutors and Kunkle's attorneys) and, noting Kunkle's money problems, fined him $550. He will not be eligible for parole and was placed on three years probation in addition to the sentence.

New York Times, 11 Jan 1989, “Former Navy Man Is Charged As a Spy”
19 Jan 1989, “Ex-Navyman Denies Trying to Sell Secrets”

***

1989 - JAMES R. WILMOTH, U.S. Navy Airman Recruit, was a food service worker aboard the carrier USS *Midway*. He was arrested by Naval Investigative Service agents in Yokosuka in July for attempting to sell classified information to a Soviet agent in Japan, where the *Midway* is based. He was tried and convicted at a general military court-martial 24 September. In addition to attempted espionage, Wilmoth was convicted of failure to report a contact with a citizen of the Soviet Union, conspiracy to unlawfully transfer classified material, and possession, use and distribution of hashish. He was sentenced to 35 years at hard labor; however, since he cooperated in the investigation, his sentence was reduced to 15 years. He

also received a dishonorable discharge, and was ordered to forfeit all his pay. He had been in the Navy for over two years and had a history of disciplinary problems including unauthorized leave of absence. Wilmoth did not have a security clearance. Classified information was procured by Petty Officer Third Class **RUSSELL PAUL BROWN** also stationed aboard the *Midway*. Brown held a Secret security clearance and took classified documents obtained from the burn bag in the electronic warfare center of the *Midway*. He passed the documents to Wilmoth, who planned to exchange the documents for cash in an arrangement with a KGB operative in Japan. Brown was convicted in October of conspiracy to commit espionage and lying to Navy investigators. A military judge sentenced him to 10 years in prison, a dishonorable discharge, reduction in rank from E-3 to E-1, and forfeiture of all pay and allowances. Motivation for the attempted sale to the Soviets was "money and greed."

Los Angeles Times, 5 Oct 1989, "Sailor Sentenced to 35 Years After Attempted Espionage"
Washington Times 5 Oct 1989, "Navy Convicts Spy, Stalks Another"
25 Oct 1989, "2nd Midway Sailor Gets Jail Term for Spying"

***

1989 - YURI N. PAKHTUSOV, a lieutenant colonel in the Soviet army, arrived in the U.S. in June 1988, as assistant military attaché with the Soviet Military Mission. Two months later he began approaching an American employee of a defense contractor to obtain documents dealing with how the U.S. government protects classified and other sensitive information contained in its computer systems. What he didn't know was that the American reported the approaches to U.S. authorities. Pakhtusov, 35, was caught as part of a sting operation after he received classified documents from the American employee working under FBI control. On 9 March 1989, he was ordered out of the country and "declared *persona non grata* for engaging in activities incompatible with his diplomatic status."

St. Louis Post-Dispatch, 11 Mar 1989, "Soviet Diplomat Ousted As Spy"

***

1989 - MICHAEL A. PERI, 22, an electronic warfare signals specialist for the Army, fled to East Germany with a laptop computer and military secrets 20 February and voluntarily returned 4 March to plead guilty to espionage. He was sentenced to 30 years in a military prison. Even after his court-martial, authorities were at a loss to explain what happened. Peri said he made an impulsive mistake, that he felt overworked and unappreciated in his job for the 11th Armored Cavalry Regiment in Fulda, West Germany. His work involved operating equipment that detects enemy radar and other signals. Peri had been described as "a good, clean-cut soldier" with a "perfect record." During his tour of duty in Germany he had been promoted and twice was nominated for a soldier of the month award.

Los Angeles Times, 29 Jun 1989, "From Soldier to Spy; A Baffling About-Face"
St. Louis Post-Dispatch, 25 Jun 1989, "U.S. Soldier Given 30 Years"

***

1989 - RONALD CRAIG WOLF, a former pilot in the Air Force from 1974 to 1981, was arrested 5 May 1989 in Dallas, Texas, for selling classified information to an FBI undercover officer posing as a Soviet agent. During his career in the Air Force, Wolf was trained as a Russian voice-processing specialist and flew intelligence missions on reconnaissance aircraft in the Far East. He held a Top Secret clearance. Discharged from the military in 1981 because of his "unsuitability for service due to financial irresponsibility," he worked as an automobile salesman for a while, but was unemployed at the time of his arrest. The FBI's investigation began in March, 1989, when information was obtained indicating Wolf's desire to sell sensitive information to the Soviet Union. Wolf talked with FBI undercover agent "Sergei Kitin" on a number of occasions thinking he was a representative of the Soviet Union assigned to

the Soviet Embassy. During these conversations Wolf talked about his military experience, and his desire to "defect" and provide Air Force secrets "for monetary gain and to get revenge for his treatment by the United States government." He was directed to mail letters to a post office box in Maryland detailing the type of information he was capable of providing. Wolf passed along classified documents concerning Top Secret signal intelligence. The FBI says they are "confident there was no exchange of information (with foreign agents) in this case." On 28 February 1990 Wolf pleaded guilty in federal court. In return for his guilty plea, the government reduced the severity of the charges against Wolf from life imprisonment to up to 10 years in prison. In June, Wolf was sentenced to 10 years without parole.

Dallas Times Herald, 1 Mar 90, "Ex-Air Force Pilot Pleads Guilty to Espionage"
Washington Post, 16 Jun 90, "Ex-Airman Get 10 Years"

***

1989 - FRANK ARNOLD NESBITT - The former Marine and Air Force communications officer was arrested by the FBI on 14 October and charged with delivering unauthorized information to the Soviet government. Nesbitt, a Memphis resident, left behind family and bewildered colleagues in June, appending a terse note to his weed trimmer ("I'm gone. Don't look for me."), and flew to Belize in Central America. Plans to settle there did not work out, so he moved on to Guatemala City where he enrolled in Spanish classes. In August while sightseeing in Sucre, Bolivia, he happened to board a bus full of Russian ballet dancers. He attended the ballet that evening and the next day bumped into a Soviet official traveling with the group. This meeting set in motion his trip to Moscow. From Sucre he went to La Paz where a Soviet embassy official arranged for his flight to Moscow. Nesbitt claims he stayed 11 days in Moscow in a safe house, wrote from memory 32 pages detailing U.S. defense communications, was polygraphed, toured the city, and met important KGB personnel. However, he grew upset over the Soviets' failure to grant him citizenship and provide him with an apartment and job. He returned, in a circuitous route, to Guatemala where he contacted U.S. authorities who then accompanied him to Washington, D.C. He was met by the FBI and arrested 11 days later. He offered his services as a double agent to the FBI claiming he did not give the Soviets any useful information. The National Security Agency, however, determined that information Nesbitt said he provided is still classified. The former communications officer served in the military between 1963 and 1966, and 1969 to 1979. On 8 November he was indicted on a charge of conspiring with a Soviet agent to pass sensitive national defense information to the Soviet Union. Nesbitt initially pleaded innocent to espionage and conspiracy charges. If convicted, he faced a possible life sentence and fines up to $500,000. According to his lawyer, Nesbitt "wanted to have some excitement in his life." A Soviet foreign ministry spokesman has said that Nesbitt was denied Soviet citizenship because a check of his autobiography he gave the Soviet parliament "led to suspicion of his possible connections with the criminal underworld." On 1 February 1990 Nesbitt changed his plea to guilty in order to receive a substantially reduced sentence. On 27 April he was sentenced in U.S. District Court to 10 years in a psychiatric treatment facility at a federal prison. His psychiatric evaluation states that he suffers from severe personality disorders.

Washington Post, 15 Oct 1989, "Odyssey of a Suspected Spy; FBI Arrests Man in Va. After Moscow Trip"
17 Oct 1989, "No Bail for Alleged Spy"
20 Oct 1989, "Suspected Spy Sought to Defect, FBI Says"
2 Feb 1990, "Guilty Plea Entered in Secrets Case"
27 Apr 1990, "Ex-Officer Given 10 Years in Mental Hospital for Spying"

***

1989 - CHARLES EDWARD SCHOOF, 20, and **JOHN JOSEPH HAEGER**, 19, both Navy Petty Officers 3rd Class, were arrested aboard ship on 1 December on charges they conspired to commit espionage. The two sailors were stationed aboard the tank landing ship USS *Fairfax County* assigned to

the Norfolk area. Both were operations specialists, trained in radar communications, electronic countermeasures, and navigational plotting. Although Schoof was reported to be the instigator, it was Haeger who had the combination to the document safe. Schoof called the Soviet Embassy in Washington, D.C. to ask if someone would come down to pick up the classified material, but Norfolk is beyond the Embassy's allowed travel radius. He then visited several bars looking for a ride to the Embassy. A shipmate reported Schoof's activities to the ship's commanding officer. It is believed that no information was passed to the Soviets and that all documents were retrieved. On 24 April 1990, Schoof was sentenced to 25 years imprisonment, stripped of all rank, forfeited all pay and allowances, and will receive a dishonorable discharge. Haeger was sentenced to 19 years, also forfeited pay and allowances and received a dishonorable discharge. Under 1987 regulations that revised parole guidelines, the two are expected to serve virtually all of their sentences.

Northern Virginia Sun, 11 Dec 1989, "Two Radar Operators From Landing Ship Charged in Spying Conspiracy"
Free Lance-Star, 26 Apr 1990, "Navy Men Get Prison Terms for Attempted Espionage"

***

1989 - DONALD WAYNE KING, Navy Airman and **RONALD DEAN GRAF**, Navy Airman Apprentice, both assigned to the Naval Air Station in Belle Chasse, LA, pleaded guilty to conspiracy to commit espionage and larceny of government property following their apprehension by Special Agents of the Naval Investigative Service. The pair was apprehended by the NIS at a motel in New Orleans after they delivered $150,000 worth of sensitive and classified aircraft parts and technical manuals to an undercover NIS agent they believed was a foreign government representative. The stolen government property and manuals (about 30 items in total) dealt with technology pertaining to the Navy's P-3 anti-submarine aircraft. The investigation was initiated in January, 1989, after an informant notified the New Orleans NIS office that King and Graf were trying to sell aircraft parts they had stolen from the Naval Station at Belle Chasse. The airmen were also charged with the sale of cocaine. King was sentenced to 10 years, reduction in rank to E-1, forfeiture of all pay and a dishonorable discharge. Graft was sentenced to 5 years, reduction in rank to E-1, forfeiture of all pay and a dishonorable discharge. Their motivation for espionage is not known; however, Graf is quoted as claiming that he did it to pay off debts amounting to $1,000.

New Orleans Times-Picayune, 5 March 1989, "2 Navy Clerks Accused of Spying"
New Orleans Times-Picayune, 7 July 1989, "Jail Terms Given in Spy Case"
Case summary provided by Albert E. DiFerderico, U.S. Naval Criminal Investigative Service

***

1990 - RODERICK JAMES RAMSAY, a former U.S. Army sergeant, was arrested in Tampa, Florida, on 7 June and charged with conspiracy to commit espionage. Ramsay joined the Army in 1981 and was transferred to West Germany in June 1983 where he was recruited by then-Army Sgt. Clyde Lee Conrad. (Conrad was sentenced to life imprisonment in May 1990 for treason.) Ramsay received $20,000 for selling military secrets that could have caused the collapse of NATO—Top Secret plans for the defense of Central Europe, location and use of NATO tactical nuclear weapons, and the ability of NATO's military communications—that were passed to Hungary and Czechoslovakia. An FBI official said, "It's one of the most serious breaches ever—it's unprecedented what went over to the other side. The ability to defend ourselves is neutralized because they have all our plans." Ramsay initially used a 35-millimeter camera to photograph classified documents, but then switched to more effective videotape. He reportedly recorded a total of about 45 hours of videotape. Ramsay is said to have a high IQ, is multilingual, and has the "ability to recall minute details, facts and figures from hundreds of volumes of documents." The FBI described him as "brilliant, but erratic." In West Germany he worked as a clerk-typist in the 8th Infantry

Division. When arrested he was unemployed, living sometimes at his mother's house and sometimes in his car. In September 1991 he pleaded guilty and agreed to cooperate with prosecutors. On 28 August 1992 he was sentenced to 36 years in prison. The sentence reflects his cooperation with investigators. According to the FBI, this case was the most extensive espionage investigation in the history of the FBI and considered to be the largest U.S. espionage conspiracy case in modern history.

Los Angeles Times 9 Jun 1990, "Alleged Spy Called Brilliant, Erratic"
Washington Times 29 Aug 1992 "Spying Sergeant Gets 36 Years"
Security Awareness Bulletin 1-97, "Profile of A Spy"

***

1991 - CHARLES LEE FRANCIS ANZALONE, a 23-year old Marine corporal stationed in Yuma, Arizona, was arrested 13 February after a four-month investigation and charged with suspicion of attempted espionage. In November 1990, Anzalone, a telephone lineman, called the Soviet Embassy in Washington to offer his services as a spy (under the pretext of asking about a college scholarship). An FBI agent posing as a KGB intelligence officer contacted Anzalone who passed him two technical manuals about cryptographic equipment, a security badge, and guard schedules. Anzalone, who is part Mohawk, told the agent that he hated capitalism, the American government, and held a grudge against the nation's treatment of native Americans. Anzalone testified that his offering to spy was a ruse to get money from the Soviets. On 3 May 1991, Anzalone was found guilty of attempted espionage. He was also convicted of adultery with the wife of another Marine stationed in the Persian Gulf, and of possession and use of marijuana. He was sentenced to 15 years in prison.

San Diego Union 2 May 1991, "Tape Shows Marine and Soviet Spy"
Los Angeles Times 4 May 1991, "Marine Guilty in Spying Case"

***

1991 - JEFFREY M. CARNEY, former intelligence specialist with the Air Force, was sentenced at a general court-martial December, 1991, to 38 years. He pleaded guilty to charges of espionage, conspiracy, and desertion. Carney entered the Air Force in December 1980. From April 1982 to April 1984 he was stationed at Tempelhof Central Airport in Berlin where he was a linguist. While at Tempelhof, he began copying classified documents which he then provided to the East German Ministry for State Security (Stasi). In 1984 he was transferred to Goodfellow AFB in Texas where he worked as an instructor while continuing to spy for East Germany. After defecting to East Germany in 1985 he continued to aid the Communists by intercepting and translating official telephone communications of U.S. military commanders and embassy officials in Berlin. Carney is a complex personality who became disillusioned with the Air Force. He originally intended to defect to East Germany, but allowed himself to be drawn into espionage by East German agents who expertly manipulated him and claimed his complete loyalty. He was apprehended in Berlin in April 1991 by Air Force OSI agents.

Cincinnati Post 21 Dec 1991, "U.S. Spy Gets 38 Years"
Air Force Times 6 Jan 1992, "Ex-Intelligence Specialist Guilty of Spying"

***

1991 - ALBERT T. SOMBOLAY, a specialist 4th class with the Army artillery, pleaded guilty in July 1991 to espionage and aiding the enemy. He was tried by military judge in Baumholder, Germany, and sentenced to confinement at hard labor for 34 years, reduction to E-1, forfeiture of all pay and allowances, and dishonorable discharge. Sombolay was born in Zaire, Africa. He became a naturalized U.S. citizen in 1978 and entered the Army in 1985 as a cannon crewman. In December 1990, assigned to

the 8th Infantry Division in Baumholder, Germany, he contacted the Iraqi and Jordanian embassies to volunteer his services in support of the "Arab cause." To the Jordanian embassy in Brussels, he passed information on U.S. troop readiness and promised more information to include videotapes of U.S. equipment and positions in Saudi Arabia. He told the Jordanians that he would be deployed to Saudi Arabia and could provide them useful information. To the Iraqi embassy in Bonn, Germany, he offered the same services, but they did not respond. On 29 December, Sombolay's unit was deployed to Saudi Arabia, as part of DESERT SHIELD, without him. Still in Germany, Sombolay continued to contact the Iraqis and provided a Jordanian representative several items of chemical warfare equipment (chemical suit, boots, gloves, and decontamination gear). His activity was discovered by U.S. Army Military Intelligence. After Sombolay's arrest in March 1991, he admitted to providing DESERT SHIELD deployment information, military identification cards, and chemical protection equipment to Jordanian officials. His motivation was money.

Cincinnati Post 7 Dec 1991, "Anatomy of a Spy"
Huntsville Times 4 Dec 1991, "Army Spy Sentenced to 34 Years"

***

1992 - JOSEPH GARFIELD BROWN, former U.S. airman and martial arts instructor, was arrested by FBI agents on 27 December 1992, and charged with spying for the Philippine government. Brown allegedly provided an official there with illegally obtained secret CIA documents on Iraqi terrorist activities during the Persian Gulf War and assassination plans by a Philippine insurgent group. The former U.S. airman was arrested at Dulles International Airport after being lured to the U.S. from the Philippines by undercover FBI agents with the promise of a job teaching self-defense tactics to CIA agents. On the following day he was indicted on three counts of espionage in federal court, Alexandria, Virginia. Brown enlisted in the U.S. Air Force in 1966 and served until 1968. He continued to reside in the Philippines, working as a martial arts instructor for the Department of Tourism until the time of his arrest. He is accused of obtaining classified documents in 1990 and 1991 in Manila from CIA secretary, **VIRGINIA JEAN BAYNES**, and passing them to a Philippine government official. An FBI spokesman stated that Baynes pleaded guilty to espionage in federal court on 22 May 1992, and served a 41-month prison term. The FBI began its investigation in April 1991 after an internal CIA inquiry determined that Baynes, who joined the agency in 1987 and who was assigned two years later to the embassy in Manila, had passed two or three classified documents to Brown. Baynes had met Brown when she enrolled in a karate class which he taught at an embassy annex. According to Baynes, as the friendship between her and Brown grew in the late summer of 1990, he asked her to obtain CIA information on assassinations planned by an insurgent group that were to be carried out in the Philippines. Baynes who held a Top Secret clearance complied with his request by removing secret documents from the embassy. Brown pleaded guilty in April 1993 to a charge of conspiring to commit espionage by delivering secret CIA documents to a Philippine government official. He was sentenced to nearly six years in prison.

Los Angeles Times, 29 Dec 1992, "Ex-U.S. Airman Charged With Espionage"
Washington Post, 6 Jan 1993, "Spy Charge Played Down by Official"

***

1992 - JEFFREY STEPHEN RONDEAU, a U.S. Army sergeant stationed at Bangor Maine was arrested in Tampa, Florida, on 22 October 1992, and charged with espionage for providing Army and NATO defense secrets, including tactical nuclear weapons' plans, to intelligence agents of Hungary and Czechoslovakia from 1985 through 1988. Rondeau was allegedly part of the Conrad spy ring which operated out of the 8th Infantry Division, Bad Kreuznach, Germany in the mid-1980s. A German court convicted former U.S. Army sergeant **CLYDE LEE CONRAD** of high treason in 1990 and sentenced him to life in prison. The inquiry into Rondeau's involvement was aided by the cooperation of

RODERICK JAMES RAMSAY. In 1991, Ramsey, also a former Army sergeant stationed in Germany, was sentenced to 36 years in prison by an American court for his involvement in the ring. As a recognition signal, Ramsay reportedly gave Rondeau a torn dollar bill to use when dealing with others in the plot. The U.S. Attorney for the Middle District of Florida said, "The espionage charge in this case is especially serious because it related to the allied defense of Central Europe including the use of tactical nuclear weapons and military communications." The three-count indictment of Rondeau charged that he conspired with Conrad, Ramsay, and others to "copy, steal, photograph, and videotape" documents and sell them to Hungary and Czechoslovakia. The indictment did not specify what amount of money he may have received. On 28 March 1994, Rondeau pleaded guilty to espionage. In June, 1994, Rondeau, along with Sgt. **JEFFERY EUGENE GREGORY**, another member of the espionage ring, was sentenced by a military court to 18 years in prison.

Houston Chronicle, 23 Oct 1992, "U.S. Soldier Is Charged With Spying"
Atlanta Constitution, 23 Oct 1992, "Soldier Accused of Selling NATO Plans to Communists"

***

1993 - STEVEN J. LALAS, a former State Department communications officer stationed with the embassy in Athens, was arrested in Northern Virginia on 3 May and charged with passing sensitive military information to Greek officials. Although Lalas originally claimed that he had been recruited by a Greek military official in 1991 and feared for the welfare of relatives living in Greece were he not to cooperate, authorities later stated that he began spying for the Greek government in 1977 when he was with the U.S. Army. It is estimated that he passed 700 highly classified documents, including papers dealing with plans and readiness for U.S. military strategy in the Balkans and a U.S. assessment of Greece's intentions toward the former Yugoslavia. Athens was Lalas' fourth communications posting with the State Department. He had previously served in Belgrade, Istanbul, and in Taiwan. During his espionage career he earned a steady income stealing, then selling, DIA reports about troop strength, political analyses and military discussions contained in cables between the U.S. Embassy in Athens and the White House, FBI communications about counter-terrorism efforts, and the names and job descriptions of CIA agents stationed overseas. Greek handlers allegedly paid him $20,000 to provide about 240 documents from 1991 to 1993. The government first learned of the espionage activities in February, 1993, when an official of the Greek Embassy here made a statement to a State Department officer indicating that he knew the contents of a Secret communication from the U.S. Embassy in Athens to the State Department. Lalas was later identified (through a video monitoring system) stealing documents intended for destruction. In June, 1993, Lalas pleaded guilty to one count of conspiracy to commit espionage and on 16 September was sentenced to 14 years in federal prison without possibility of parole. Prosecutors had recommended the 14-year sentence in return for Lalas' promise to reveal what documents he turned over and to whom. The full extent of his espionage activity was revealed prior to sentencing only after he failed two FBI polygraph examinations. Lalas, 40, is of Greek descent, but was born in the U.S.

Washington Post, 4 May 1993, "Va. Arrest Made in a Spy Case From Greece"
New York Times, 4 May 1993, "Am. Employee at Embassy in Athens Arrested as Possible Spy"
New York Times, 6 May 1993, "U.S. Embassy Employee Sold Secrets to Greeks, F.B.I. Says"
Washington Post, 16 Sep 1993, "A 14-Year Sentence for Selling Secrets"

***

1993 - GENEVA JONES, a secretary with a top-secret clearance in the State Department's Bureau of Politico-Military Affairs was arrested 3 August and indicted 31 August for theft of government property and transmission of defense information to unauthorized persons. FBI agents say she smuggled classified documents for two years to West African journalist **DOMINIC NTUBE**, indicted at the same time. Jones

was carrying classified government documents with her at the time of arrest. Agents who searched Ntube's Washington, D.C. apartment after his arrest on 4 August found thousands of classified cables and 39 CIA documents marked Secret including documents relating to U.S. military operations in Somalia and Iraq. Some of the material apparently made its way to West African magazines, which had been publishing classified State Department cables for several months. Agents indicated they wire-tapped Jones' phone after several classified U.S. documents were found 10 months earlier in the West African command post of Charles Taylor, leader of a violent movement to overthrow the Liberian government. Ntube reportedly faxed 14 documents he received from Jones to the Liberian rebels. The former State Department employee told the FBI she had been giving Ntube classified cables for about 18 months. In a preliminary hearing, the FBI testified that agents watched her on 16 occasions take documents from the department and hide them in newspapers or a grocery bag. During the month she was under surveillance, she allegedly took more than 130 classified documents from her office. On 31 August, Ntube was indicted with Jones for receiving stolen property and for transmitting national defense information to unauthorized persons. In June, 1994, Jones pleaded guilty to 21 counts of theft and two counts relating to the unlawful communication of national defense information. In delivering a sentence of 37 months in prison (longer than what the prosecution had asked), U.S. District Judge Harold H. Greene stated, "Somebody would have to be a complete moron not to know that when you work for the State Department you can't take documents out and give them to anybody." A trial date has not been set for Ntube..

Washington Post, 5 Aug 1993, “FBI Arrests Two in Theft of State Dept. Documents”
Washington Post, 31 Aug 1993, “Two Indicted in Theft of State Department Documents”

***

1993 - FREDERICK CHRISTOPHER HAMILTON, a former Defense Intelligence Agency official, pleaded guilty on 5 February 1993, to the charge of passing to Ecuadorian officials classified U.S. intelligence reports evaluating the military readiness of Peruvian security forces. At the time, Hamilton was a DIA research technician in the defense attaché’s office in Lima, Peru, a post which he held from 1989 to 1991. He apparently believed that the disclosures could help avert a possible conflict between the two countries. Peru and Ecuador have been disputing territory (sometimes violently) along their mutual border for the past 50 years. Hamilton holds advanced degrees in Spanish and Portuguese. At the time of his arrest, he was employed as a language instructor at a military academy in Virginia. His activities were uncovered by U.S. intelligence agencies after receiving information from a confidential source indicating secrets were being leaked. Hamilton, who held a Top Secret security clearance while with the DIA, met Ecuadorian representatives in their embassy in Lima on 13 February and 20 May of 1991. He passed extremely sensitive information which disclosed U.S. intelligence operations and the identity of U.S. sources in the region. “He didn't get any money,” said a U.S. official. “He was a very naive individual who was flattered by the [Ecuadorians].” Hamilton's attorney stated that, “What he thought he was trying to do was prevent a war... The purpose of disclosing the documents that he did was to show the country that was concerned about being attacked that the other country had neither the intent nor the ability to attack.” Hamilton reportedly passed five Secret intelligence reports and orally disclosed the contents of four other classified reports. Under a court agreement, the former DIA employee pleaded guilty to two counts of unlawfully communicating classified information to a foreign country. The agreement specifies Hamilton may not appeal the sentence and the Justice Department will not prosecute him for espionage-related crimes. On 16 April, he was sentenced to 37 months in prison.

The Washington Post, 6 Feb 1993, “Va. Man Pleads Guilty to Leaking U.S. Secrets”
The Washington Times, 6 Feb 1993, “Ex-DIA Official Pleads Guilty in Document Leak”

***

1993 - JEFFERY E. GREGORY a U.S. Army Staff Sergeant was arrested 29 April 1993, at Fort Richardson, Alaska, resulting from a joint investigation between the FBI and the U.S. Army Intelligence and Security Command. As of this date he is the sixth active or former U.S. service member charged with espionage in connection with the Conrad/Szabo espionage network that sold U.S. and NATO military secrets to Hungary and Czechoslovakia when those countries were in the Soviet Bloc. Gregory is alleged to have been a member of the spy ring which operated out of the 8th Infantry Division, Bad Kreuznach, Germany in the mid-1980s. German authorities convicted former U.S. Army sergeant **CLYDE LEE CONRAD** of high treason in 1990 and sentenced him to life in prison. In 1991, another ring member **RODERICK JAMES RAMSAY**, also a former Army sergeant stationed in Bad Kreuznach, was sentenced to 36 years in prison by an American court for his involvement in the network. Clyde Conrad recruited Ramsay to the spy ring who is believed to have recruited others, including Gregory. According to the federal complaint against Gregory, while assigned to the 8th Infantry Division in Germany from March 1984 to October 1986, "he helped procure extremely sensitive, classified documents relating to national defense, for transmittal to one or more foreign powers." At that time, Gregory was a staff driver at Bad Kreuznach, West Germany, and helped maintain the commanding general's mobile command center. He was also in charge of updating maps showing military maneuvers and had access to classified messages and correspondence. According to an FBI official, Gregory once took a military flight bag stuffed with 20 pounds of classified documents. The documents included "war plans" for the U.S. and NATO. On 28 March 1994, Gregory pleaded guilty to espionage charges. In June, 1994, Gregory, along with Sgt. **JEFFREY STEPHEN RONDEAU**, another member of the espionage ring, was sentenced by a military court to 18 years in prison.

New York Times, 2 May 1993, "Fourth Army Sergeant Held in Espionage Case"
Huntsville Times, 2 May 1993, "4th Army Sgt. Arrested in Alleged Espionage Ring in Germany"

***

1993 - YEN MEN KAO, a Chinese national, residing in Charlotte, North Carolina, was arrested on 3 December 1993, after a six-year investigation into a spy ring that sought secrets on advanced naval weapons and technology. According to an official statement, Kao "and several other Chinese nationals" conspired to illegally procure and export classified and embargoed high-technology military items. Kao was also charged with violating U.S. immigration laws. Targeted for illegal export were the Navy's MK 48 Advanced Capability (ADCAP) Torpedo, two F 404-400 General Electric jet engines used to power the Navy's F/A-18 Hornet fighter, and fire-control radar for the F-16 Falcon jet. Although these systems were not delivered to China, Kao was able to transfer embargoed oscillators used in satellites for which Kao paid an FBI informant $24,000 as part of a sting operation. On 22 December, an immigration judge ordered Yen Men Kao's deportation to Hong Kong for overstaying his visa and for "committing acts of espionage against the United States." A decision was made not to prosecute to avoid offending the Chinese government and to protect counterintelligence sources and methods that might have been disclosed in court. Kao who reportedly owned two Chinese restaurants in Charlotte, had been under FBI surveillance for several years. During this time he met and received instructions from Chinese intelligence agents who offered him $2 million to obtain U.S. weapons technology. According to one federal official, Kao had a gambling problem and lost money supplied by his Chinese handlers. Fearing reprisal from the Chinese as well as the U.S., he requested deportation to Hong Kong rather than mainland China. According to a senior FBI official, an investigation into the technology acquisition scheme is continuing and more arrests may be made. Kao leaves behind his wife, a naturalized U.S. citizen and two children.

Washington Times, 22 Dec 1993, "Spy Sting Gets Chinese Man Deported"
Los Angeles Times, 5 Dec 1993, "FBI Arrests Chinese National in Spy Ring Investigation"

***

1994 - ALDRICH HAZEN AMES, CIA intelligence officer and his Colombian-born wife **MARIA DEL ROSARIO CASAS AMES**, were arrested 21 February , after a 10-month investigation, on charges of providing highly classified information to the Soviet KGB and later, to its successor, the Ministry of Security for the Russian Federation (MBRF) over a nine-year period. From 1983 to 1985, Ames was assigned to the CIA's counterintelligence branch in the agency's European Division and was responsible for directing the analysis of Soviet intelligence operations. In this capacity he would have known about any penetration we had of the Soviet military or the KGB. According to press reports, the trail that led to the arrest of Ames and his wife began in 1987 after the unexplained disappearance or deaths of U.S. sources overseas. According to court documents, Ames's information allowed the Russians to close down at least 100 intelligence operations and at least 10 U.S. and allied agents were executed. Ames reportedly received up to $2.5 million from his Russian handlers over this period of time. Reports of the Ameses' high-rolling life style included the cash purchase of a half-million dollar home, credit card bills of $455,000, and new Jaguar sports car. A search of his office uncovered 144 classified intelligence reports not related to his current assignment in CIA's Counternarcotics Center. Consequently some fear exists that Ames may not have acted alone within the agency. On 28 April, Aldrich Ames and his wife pleaded guilty to conspiring to commit espionage and to evade taxes. Ames was immediately sentenced to life imprisonment without parole. Under the plea agreement, Maria Rosario Ames was sentenced to five years and three months in prison for conspiring to commit espionage and evading taxes on $2.5 million obtained by her husband for his illegal activities.

New York Times, 22 Feb 1994, “Ex-Branch Leader of C.I.A. is Charged as a Russian Agent”
Washington Post, 23 Feb 1994, “CIA Officer Charged With Selling Secrets”
Washington Post, 25 Feb 1994, “Accused Couple came from Different Worlds”
Los Angeles Times, 22 Oct 1994, "Wife of CIA double agent sentenced to 5 years in prison"
Washington Post, 27 Dec 1994, "Ames says CIA does not believe he has told all"
Security Awareness Bulletin, 4-94, “An Assessment of the Aldrich Ames Espionage Case”

***

1994 - MICHAEL SCHEVITZ, American professor, resident and employed in Germany since the 1970s, was convicted by a German court in November 1995 for having worked for the East German intelligence organization (*Stasi*) from 1977 until early 1990. During this time he reportedly received $23,000 for information provided on personal information about West German scientists that would have made them vulnerable to recruitment for espionage. Schevitz was employed as a social policy analyst at Germany's Nuclear Research Center in Karlsruhe. His name surfaced in the files of the former Ministry for State Security when they were opened to Western intelligence services in 1993. Schevitz, who had taken part in the UC-Berkeley protests of the 1960s, claimed that he had been working for the CIA at the time, a story repeatedly denied by that agency. The German magistrate in stating that the American sociologist had not done "any measurable harm," gave Schevitz an 18-month prison term, reducing it immediately to three years probation and ordered the professor to pay $10,000 to a German charity.

Los Angeles Times, 11 Nov 1995, "U.S. Professor Guilty in German Spy Case"

***

1995 - JOHN DOUGLAS CHARLTON, retired Lockheed Corporation engineer, was arrested on 25 May for attempting to sell secret documents removed from the company at the time of his retirement. According to an Assistant U.S. Attorney, the plans concerned the *Sea Shadow*, a Navy stealth project and the *Captor Project* related to mines which release anti-submarine torpedoes. According to the 10-point espionage indictment, Charlton tried to sell the information to an FBI agent posing as a foreign government representative. Five times between July and September 1993, Charlton attempted to sell the secrets for $100,000 to the undercover agent. Charlton joined Lockheed in Sunnyvale, California, in 1980 as a research specialist and left the company under an early retirement program in 1989, but

apparently was disgruntled about the circumstances of his departure. At the time of his retirement he took with him several classified documents outlining U.S. defense projects. A search of his Lancaster, California, residence turned up a cache of illegal guns and the classified documents. Following a plea agreement on 17 October, Charlton pleaded guilty to selling two classified schematic drawings related to the anti-submarine program. He admitted knowing that the *Captor Project* information which the former engineer attempted to sell to what he believed to be a French official was highly classified. According to the prosecuting attorney, "The documents would have enabled any nation to discover some of the workings of the program." On 8 April 1996, Charlton was sentenced to 2 years in federal prison and fined $50,000 for his guilty plea to two counts of attempted transfer of defense information. He will be placed on five years probation after his release. He is not eligible for parole.

Los Angeles Times, 26 May 1995, "Ex-Aerospace Worker Indicted In Spy Case"
Antelope Valley Press (California), 18 Oct 1995, "Valley Man Pleads Guilty To Attempted Espionage"
Los Angeles Times, 10 Apr 1996, "Retired Engineer Gets 2 Years in Defense Espionage Case"

***

1995 - MICHAEL STEPHEN SCHWARTZ, U.S. Navy Lt. Cmdr., was charged with passing Department of Defense classified documents and computer diskettes to Saudi naval officers between November, 1992, and September, 1994, while assigned to a U.S. military training mission in Riyadh, Saudi Arabia. Schwartz, a naval surface warfare officer who served in the Gulf War, was charged with four counts of espionage on 23 May. He is also charged with five counts of violating federal regulations for allegedly removing classified material to his residence. The charges result from a Naval Criminal Investigative Service investigation which began in September, 1994. The documents allegedly included classified messages to foreign countries, military intelligence digests, intelligence advisories, and tactical intelligence summaries classified up to the SECRET (NOFORN) level. There is no indication that Schwartz received any money for the materials; according to a media report, Schwartz was attempting to be helpful to the Saudis because of U.S.-Saudi cooperation during the Gulf War. On 14 October, Schwartz agreed to a plea bargain that allowed him to avoid a court-martial and possible imprisonment. According to the agreement, in November, 1995, Schwartz received an "other than honorable" discharge and lost all retirement benefits and other military privileges.

The Virginian-Pilot (Norfolk VA), 25 May 1995, "Officer Spied for Saudis, Navy says"
Washington Jewish Week, 1 Jun 1995, "Navy Officer Arrested On Charges Of Espionage"
Washington Post, 13 Sep 1995, "Norfolk Naval Officer Faces Court-Martial in Espionage Case"
The Virginian-Pilot, 14 Oct 1995, "Navy Officer Accused of Spying Gives Up Retirement Benefits"

***

1995 - ALURU J. PRASAD and **SUBRAHMANYAM KOTA:** On October 8th, Indian businessman, Aluru J. Prasad, and ten days later, software engineer Subrahmanyan Kota were arrested and detained for their involvement in a spy ring that sold highly sensitive defense technology to the KGB between 1985 and 1990. Prasad, a wealthy Indian national, who frequently visited the United States, was alleged to have been an agent of the KGB. Kota, a naturalized U.S. citizen was president of the Boston Group computer consulting firm. According to an FBI affidavit, the pair met Russian agents in Bermuda, Portugal, Switzerland, and other foreign locations and at these meetings passed classified defense information. At the time of their indictment, it was revealed that Kota and another conspirator, Vemuri Reddy, had been arrested the previous December by FBI agents, posing as Russian intelligence agents, to whom they had attempted to sell (for $300,000) micro-organisms used in the production of a high-tech drug. Beginning in 1989, Prasad plotted with Kota of Northborough, Massachusetts, and other unnamed persons to obtain classified technology from a network defense contractor employees. Prasad and Kota specifically sought information about mercury cadmium telluride missile detectors, radar-absorbing coating used on stealth fighters and bombers, and semiconductor components used in infrared missile-

tracking systems. According to their indictment, the two received $100,000 for information about each project. On October 29th, 1996, former KGB intelligence officer Vladimir Galkin was arrested as he attempted to enter the United States at Kennedy Airport in New York. Galkin was alleged to have been Kota and Prasad's contact with the KGB and met with Kota in Cyprus beginning in late 1990. Although Galkin had not committed espionage on American soil, he was charged for his involvement in the conspiracy. In June, 1996, under a plea agreement, Kota pleaded guilty to selling stolen biotech material and evasion of income taxes and agreed to testify against Prasad. He admitted that he was paid a total of $95,000 by Prasad and his alleged KGB colleagues. Prasad's first trial ended in a mistrial; however, in a second trial in December 1996 he was convicted of espionage charges. Under a plea agreement Prasad was sentenced to the 15 months he had served awaiting his trial and agreed to return to India. On November 13th accused KGB intelligence Vladimir Galkin was released.

Boston Globe, 19 Oct 1995, "Northborough Man Charged With Espionage"
Boston Globe, 12 Jun 1996, "A Post-Cold War Spy Story Comes To Life"
Washington Times, 5 Nov 1996, Computer Check of Visa at Airport IDs Spy Suspect"

***

1996 - KURT G. LESSENTHIEN, Navy petty officer, arrested in Orlando, Florida, on April 3rd was charged with attempted espionage after offering information about nuclear submarine technology to a Russian government representative. Lessenthien was subsequently contacted by undercover agents of the FBI and Naval Criminal Investigative Service posing as Russian agents. At the time Lessenthien was an instructor at the Navy Nuclear Power School in Orlando and was very knowledgeable about the design and operation of submarine motors. It was reported that the petty officer, in a phone call to the Russian embassy, offered Top Secret information about the movement of U.S. submarines in exchange for thousands of dollars. According to one media source, Lessenthien accumulated nearly $25,000 in credit card debt on a "relentless pursuit of women" that he intended to marry. A Navy psychiatrist testified that he suffered personality flaws that drove him to ruin an excellent military record. However, a Navy prosecutor stated that Lessenthien decided to become a spy for money and excitement, not love, and that the petty officer had been storing classified materials since 1991. On October 28, Lessenthien was sentenced by a military court to life imprisonment, but will serve 27 years under a plea agreement. He was also given a dishonorable discharge and ordered to forfeit all pay and benefits.

Washington Post, 4 Apr 1996, "Petty Officer Arrested on Spy Charges"
Orlando Sentinel, 24 Apr 1996, "Orlando Sailor In Spy Arrest."
Virginian-Pilot (Norfolk), 29 Oct 1996, "Lessenthien Gets 27 Years In Espionage Case"

***

1996 - PHILLIP TYLER SELDON, former Pentagon civilian employee pleaded guilty on August 7th in Alexandria to passing classified documents to a Salvadoran air force officer while on active military duty in El Salvador as a U.S. Army captain. After leaving the Army, Seldon took a civilian job with the Department of Defense. According to court documents, Seldon gave the Salvadoran three packets of documents between November 1992 and July 1993. None of the material was reported to have exceeded the Secret level. Seldon claimed that he had met the Salvadoran officer while working as an intelligence advisor, and he believed that the officer had the appropriate clearance. This information came to light in the course of a polygraph examination as Seldon was applying for a position with the CIA. On November 8th, Seldon was sentenced by a U.S. District court to two years in prison.

Washington Post, 9 Nov 1996, "Ex-Pentagon Worker Given 2 Years For Passing Secrets"

***

1996 - ROBERT STEPHAN LIPKA, former National Security Agency staff member, was taken into custody on February 23 at his home in Millersville, Pennsylvania, and charged with committing espionage while workings as a communications clerk from 1964 to 1967. While a Army enlisted man between the ages of 19 and 22, Lipka worked in the NSA central communications room and reportedly provided the KGB with a constant stream of highly classified reports. He is believed to have caused extensive damage to U.S. intelligence collection activities. According to the James Bamford writing in the *Los Angeles Times*, since Lipka provided Top Secret information to the KGB during the war in Vietnam, he may have been responsible for the loss of American lives. He is said to have used dead drops along the C&O Canal near the Potomac River and was paid between $500 and $1000 per delivery. Lipka left the NSA in 1967 and stopped meeting with his KGB handlers in 1974. He became a suspect in 1993 as a result of information believed to have been provided to the FBI by his ex-wife. His role in espionage was confirmed by FBI agents posing as Russian contacts. According to an FBI spokesman, while the government was aware of a major security breach in the 1960s, it had not been able to identify Lipka as a suspect until it had received the additional information. It is believed that Lipka is the young soldier described in the autobiography of former KGB major general Kalugin who tells of a walk-in in the mid-1960s who was interested in money. According to Kalugin, the documents which the soldier passed included top secret NSA reports to the White House and copies of communications on U.S. troop movements around the world. The price reportedly paid by the Soviets during the period of his betrayal was $27,000. On May 23, 1997, Robert Lipka pleaded guilty to one count of espionage in exchange for a jail term of no more than 18 years. A sentencing date is set for August 15, 1997.

Washington Post, 24 Feb 1996, "FBI Arrests Ex-Soldier As Mysterious KGB Spy In Supersecret NSA"
Los Angeles Times, 3 Mar 1996, "Has A 30-year Mystery Unraveled?"
Wall Street Journal, 21 Nov 1996, "How the FBI Broke Spy Case That Baffled Agency For 30 Years"
Baltimore Sun, 24 May 1997, "Ex-clerk at NSA Is Guilty Of Spying; Former Soldier Sold Secret Documents To Soviets In Mid-1960s"

***

1996 - HAROLD J. NICHOLSON, was arrested on November 16th at Dulles International Airport as he was about to board a flight to Switzerland. On his person were found rolls of film bearing images of Top Secret documents. Nicholson is the highest ranking Central Intelligence Agency officer (GS-15) charged with espionage to date. Counterintelligence officials believe that he began spying for Russian intelligence in June 1994 as he was completing a tour of duty as deputy station chief in Malaysia. He joined the agency in 1980 after serving as a captain in the U.S. Army. He was charged with passing a wide range of highly classified information to Moscow including biographic information on every CIA case officer trained between 1994 and 1996 and highly sensitive counterintelligence information, including a summary report of interviews with Aldrich Ames following his arrest. He is also suspected of having compromised the identities of U.S. and foreign business people who have provided information to the CIA. According to investigators, for two and a half years he had been hacking into the agency's computer system and providing the Russians with every secret he could steal. It is alleged that Nicholson received approximately $120,000 from the Russians over a two-year period. He came under suspicion in late 1995 when he failed a series of polygraph examinations. Further investigation revealed a pattern of extravagant spending, and an unusual pattern of foreign travel followed by large, unexplained bank deposits. Nicholson, who at the time was in the middle of a divorce and child custody battle, claimed that he did it for his children and to pay his bills. On November 21st he was indicted on one count of conspiracy to commit espionage. On March 3rd, 1997, Nicholson pleaded guilty under a plea agreement in which he admitted that he had been a Russian spy. On June 6th he was sentenced by a Federal judge to 23 years and 7 months in prison, which reflected his extensive cooperation with government investigators.

Los Angeles Times, 19 Nov 1996, "Career CIA Officer Is Charged With Spying For Russia"

Los Angeles Times, 21, Nov 1996, "Alleged Mole To Plead Not Guilty"
Washington Post, 6 Jun 1997, "Convicted Spy Says He Did It For His Family"
New York Times, 4 Mar 1997, "C.I.A. Officer Admits Spying For Russians"

***

1996 - EARL EDWIN PITTS, a senior FBI agent, was arrested on December 18th at the FBI Academy in Quantico, Virginia, and charged with providing classified information to the Russian intelligence services from 1987 until 1992. He is believed to have received $224,000 from Russian intelligence services for his activities. Pitts allegedly turned over top secret documents to the KGB (and after the collapse of the Soviet Union, the SVRR) including a list of FBI assets who were providing intelligence on Russia. Pitts' betrayal of trust began in July 1987 when, as a newly assigned agent to the New York City field office, he wrote to a Soviet representative assigned to the Soviet mission at the United Nations and asked to meet a KGB officer. From 1988 to 1992 Pitts allegedly made nine brief trips to New York to provide documents to his handler, KGB officer Aleksandr Karpov. Each trip was followed by an unexplained deposit in one of several bank accounts in the Washington area. After 1992 Pitts became inactive as a foreign agent. He was identified as a mole when Karpov himself became a double agent for the FBI. At this time the FBI set up a sting operation against Pitts and, using agents posing as Russians, easily gained his agreement to renew his espionage activities. Over a period of 15 months, Pitts made 22 drops of classified documents to undercover FBI agents and was paid $65,000. The Bureau was also informed of Pitts' involvement by his wife, Mary Colombaro Pitts who confided her suspicions about her husband's activities to another FBI agent. Earl Edwin Pitts pleaded guilty to two counts of espionage in February 1997 following the discovery of a computer disk with a letter to his Russian handler. On June 23rd, he was sentenced to 27 years in prison by a Federal judge who stated that the former agent was guilty of "the most egregious abuse of trust." When asked why he spied, Pitts cited a number of grievances he had against the FBI and stated that he "wanted to pay them back."

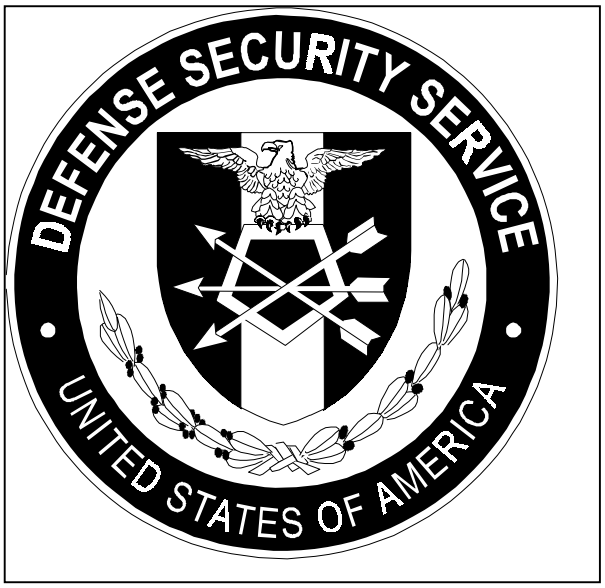
Washington Post, 19 Dec 1996, "Senior FBI Agent Charged With Spying For Russians" and "Espionage Suspect Depicted As Eager To Sell His Loyalty"
Washington Post, 2 Mar 1997, "Spy Case Sealed By 1990 Letter; Computer Disk Held Agent's Memo to KGB"
Washington Post, 24 Jun 1997, "Ex-FBI Agent Gets 27 Years For Passing Secrets To Moscow"

***

1996 - ROBERT C. KIM, a Navy civilian computer specialist, working at the Office of Naval Intelligence in Suitland, Maryland, was charged on September 25th with passing classified information to a foreign country. He was arrested outside a diplomatic reception at Ft. Myer, Virginia, on September 24th as he stood beside Capt. Baek Dong-Il, a Korean Embassy Naval attaché and the alleged recipient of the classified materials. Kim, a native of Korea, became a U.S. citizen in 1974 and has lived in the United States for 30 years. He had access to classified information since 1979. According to investigators, over a five month period, he passed dozens of classified documents (including some which were Top Secret) out of loyalty to his country of birth. An FBI affidavit states that Kim searched naval computer systems, made copies of sensitive classified intelligence reports, removed classified markings, printed them off, and mailed or passed them in manila envelopes to Baek. The documents included military assessments about North Korea and China, and U.S. intelligence assessments of South Korean government officials. In his official capacity, Kim operated a computer program that tracked global shipping movements. However, he had access to highly classified documents from other intelligence agencies. Kim came under surveillance by the Naval Investigative Service when it learned of his contact with Baek. A court-approved search of Kim's office produced a list of classified documents he had illegally passed to the naval attaché. More than 40 documents sent to Baek were intercepted in the mail. Capt. Baek Dong-Il who enjoyed diplomatic immunity was subsequently recalled by his government. While there is no evidence that Kim received any payment for his illegal activities, according to one

news source, he had requested assistance from the South Koreans in his efforts to find employment with a South Korean intelligence or customs agency after his retirement from his U.S. Navy job. It is also reported that Kim had accumulated a credit card debt of approximately $100,000. On May 7th, 1997, Robert C. Kim pleaded guilty to one count of conspiracy to commit espionage. Sentencing is set for July 11. The former Navy employee faces a maximum punishment of 10 years in prison.

Washington Post, 26 Sep 1996, "Navy Worker Is Accused Of Passing Secret; Papers Allegedly Went To S. Korean Officer"
Washington Post, 2 Oct 1996, "Kim Allegedly Sought Job With S. Korea"
Los Angeles Times, 8 May 1997, "Ex-Analyst Admits Spying For S. Korea In Plea Bargain"


DEFENSE SECURITY SERVICE
UNITED STATES OF AMERICA

HOW TO REVIEW CREDIT BUREAU REPORTS

The Credit Report designed for DSS use is divided into two parts:

1) Report of Credit Summary Page (displays a summary of accounts, including high credit, past due summaries, repossessions, liens, judgments, etc)

2) DSS Detailed Report of Credit (displays a detailed listing of each credit account)

This reference document provides a sample of a typical report and highlights areas using legends ◯to help identify and define entries.

CREDIT REPORT SUMMARY PAGE

REPORT OF CREDIT	DATE	NAC CASE No	DCCS CASE NO
	10/13/98	999990041	99999DQ132241M2

0001	Social Security Number	Date of Birth	
	123-45-6789	28 FEB 68	

(1) **Subjects Name:** CHEESE, CHUCK E.
AKA #1:
AKA #2:
AKA #3:
AKA #4:
AKA #5:

REVIEW OF CREDIT BUREAU RECORDS DISCLOSED - SEE ATTACHED (2)

NUMBER OF DSS 1 (3)

CREDIT REPORT SUMMARY

REPORTED FACTORS

REPORTED MORTGAGE BALANCE OWED	$0	(4)	DEBT CONSOLIDATION	(Y/N)	N	(9)
REPORTED BLNC OWED (EXCLD MRTG)	$6.835	(5)	CHECK RETURNED	(Y/N)	N	(10)
REPORTED PAST DUE	$217	(6)	CONSUMER COUNSELING	(Y/N)	N	(11)
TOTAL NUMBER OF OPEN ACCOUNTS	3	(7)	CANNOT LOCATE	(Y/N)	N	(12)
HIGH CREDIT (EXCLD MRTG)	$15.902	(8)	CONTACT MEMBER	(Y/N)	N	(13)

(14)	#ACCTS	LIABILITY
30 DAYS PAST DUE	1	$200
60 DAYS PAST DUE	0	$0
90 DAYS PAST DUE	0	$0
120 DAYS PAST DUE	0	$0

	#ACCTS	LIABILITY	
REPOSSESSION	0	$0	(15)
COLLECTION/CHARGE OFF	3	$395	(16)
LIENS/JUDGEMENTS	3	$2.926	(17)
GARNISHMENT	0	$0	(18)
BANKRUPTCY	0	$0	(19)
INCLUDED IN BANKRUPTCY	0	$0	(20)
FORECLOSURE(S)	0	$0	(21)

PREVIOUS HISTORY

(22)	#ACCTS
30 DAYS PAST DUE	0
60 DAYS PAST DUE	2
90 DAYS PAST DUE	1
120 DAYS PAST DUE	1

Reported repossession, collections, liens, judgements, garnishments, etc. May include accounts which have been satisfied. In addition the liability amounts may be included in * Reported Past Due *

WARNING

(23) 444 / 888 / / / / / / / / / / / / / / / / / / | * *

CREDIT REPORT SUMMARY PAGE
LEGEND

① **SUBJECT'S NAME AND AKA's** – These are the names included on the Subject's PSQ that DSS submitted to the credit vendors. This segment does not include any additional AKAs or name variations returned by the credit vendors. If reported by the credit vendors, those are listed in the personal information section on the last page of the full credit report.

② **BRIEF DESCRIPTION OF THE CREDIT INFORMATION OBTAINED** –
One of the following statements is printed:

(1) REVIEW OF CREDIT BUREAU RECORDS DISCLOSED – SEE ATTACHED

(2) REVIEW OF CREDIT BUREAU RECORDS DISCLOSED – SEE INFORMATION BELOW

(3) REVIEW OF CREDIT BUREAU RECORDS DISCLOSED – NO CREDIT INFO. ON FILE

- Statement (1), above, is printed if either the computer indicates that the DSS financial issue case decision logic table (DLT) threshold may have been met[1] or if one or more potentially significant issues not considered by the DLT were noted in the text of the full credit report. Examples of the latter include statements that indicate that the Subject may have been reported deceased, received a government fine, broke a lease, etc.

- Statement (2), above, is printed when at least some credit or prior inquiry information is obtained from the credit vendor and neither condition required for printing statement (1) was present.

- Statement (3), above, is printed when the credit vendor(s) checked reported that they had absolutely no credit history or only credit report inquiry information on file for that Subject.

③ **NUMBER DSS CREDIT INQUIRIES** – The number printed indicates the number of credit history files DSS requested for that Subject. The number will vary depending upon where the Subject lived and how may AKAs DSS decided to search under. In certain instances it will be necessary to pull credit information from more than one vendor because no single credit vendor can provide adequate coverage for all the locations that need to be covered. When multiple credit histories are purchased, the information is drawn together, duplicate entries, removed and the findings are printed and summarized on a single credit report.

[1] Human verification that the DSS financial issue case Decision Logic Table (DLT) threshold has actually been met is necessary because of possible duplicate entries. Although the computer program will remove most of the duplicate credit account entries pulled from the credit vendors, in some instances this will not be possible. Duplicates will occur when the names of the lender or some other piece of critical information pertaining to those accounts is reported differently by the credit vendors supplying that information. Therefore, certain accounts might be counted more than once toward meeting the DLT. The computer program making this assessment is designed to err on the conservative side when dealing with these issues.

CREDIT REPORT SUMMARY PAGE
LEGEND

④ **REPORTED MORTGAGE BALANCE OWED** – The dollar value shown reflects the sum of the balances owed (as opposed to either past due or the original amount borrowed) for all accounts that have been designated as mortgage accounts on the credit report. Home equity and all other accounts that are not specifically designated by the credit history vendors as mortgage accounts are treated as regular accounts and their values are not included in this total. It should be noted that not all lenders provide credit history vendors with loan or mortgage information.

⑤ **REPORTED BALANCE OWED (EXCLUDING MORTGAGES)** – The dollar value presented reflects the sum of the balances owed for all accounts except those designated as mortgage accounts. If closed accounts, paid installment accounts or charge–off accounts still indicate a balance owed, those values will be included in this total.

⑥ **REPORTED PAST DUE** –The dollar value displayed reflects the sum of the past due segment for all accounts (including mortgages). If closed accounts, paid installment accounts or charge–off accounts still list a past due amount, they will be included in this total.

⑦ **TOTAL NUMBER OF OPEN ACCOUNTS** – The number shown reflects the total number of trade accounts (i.e., accounts with lenders) contained on the credit report that have not been specifically designated as closed accounts. This total includes paid installment accounts, revolving credit accounts that have not been used recently, charge–offs and all other trade accounts that have not been designated as closed.

⑧ **HIGH CREDIT (EXCLUDING MORTGAGES)** – The value presented is the sum of the high credit amounts shown on all trade accounts except mortgages. If closed accounts, paid installment accounts or charge–off accounts still list high credit amounts, those amounts will be included in this total. In certain cases the amount owed on a revolving account is more than the high credit value shown. Even in those cases the amount reflected in the total would be the high credit value reported for that account.

⑨ **DEBT CONSOLIDATION (Y/N) –** A "Y" for yes is printed whenever at least one statement appears in the text of the credit report that the Subject has undergone formal debt consolidation.

◯ **CHECK RETURNED (Y/N)** – A "Y" for yes is printed whenever at least one statement appears in the text of the credit report that the Subject has checks returned for insufficient funds.

◯ **CONSUMER COUNSELING (Y/N)** – A "Y" for yes is printed whenever at least one statement appears in the text of the credit report that the Subject has undergone formal consumer counseling.

◯ **CANNOT LOCATE (Y/N)** –A "Y" for yes is printed whenever at least one statement appears in the text of the credit report that a lender was unable to locate the Subject who had an outstanding loan with that firm.

CREDIT REPORT SUMMARY PAGE
LEGEND

⑬ **CONTACT MEMBER (Y/N)** – A "Y" for yes is printed whenever at least one statement appears in the text of the credit report that a lender wants interested parties to contact them for credit information about that Subject.

⑭ **CURRENT PAST DUE TABLE** – This table reflects the number of accounts that are currently being reported as 30 or more days past due in the manner of payment segment. It does not include accounts whose manner of payment segment indicates bad debt, collection or paid as agreed (even if there is a past due amount indicated for the account). Accounts whose manner of payment is 120, 150, or 180 days past due are reported under the 120 days past due (the maximum value contained on that table). The liability segment of the table reflects the past due sum of all the accounts whose manner of payment is reported at that level.

⑮ **REPOSSESSION –** The number of repossessions and the sum of the balance due segments for all these accounts is reflected on this line.

⑯ **COLLECTION/CHARGE OFF** – The number of collections and charge-offs and the sum of the balance due segment for these accounts is reflected on this line. If the balance due segment equals zero, the high credit segment may be listed in the liability column. Accounts whose manner of payment is listed as "bad debt" that do not involve repossessions, bankruptcies or foreclosures are included.

⑰ **LIENS/JUDGEMENTS** – The number of public records that pertain to liens or judgments and the sum of the liability segments for these accounts are reflected on this line. If multiple liens and judgments are present, some of them may be counted more than once. Only liens or judgments having the same docket number as an existing entry are deleted by the computer (the public record with the most recent filing date is kept). Satisfied liens and judgements are included in the number total and will be included in the liability total if there is a liability balance still indicated.

⑱ **GARNISHMENT** – The number of garnishments (including wage assignment accounts) and the sum of the balance due segments for these accounts is reflected on this line.

◯ **BANKRUPTCY** – The number of public records that pertain to bankruptcies and the sum of the balance due segments for these accounts is reflected on this line. If multiple bankruptcy records exist a single bankruptcy may be counted more than once.

Only bankruptcy records having the same docket number as an existing entry are deleted by the computer (the public record with the most recent filing date is kept). Dismissed, filed, completed and discharged bankruptcy records are included in the number total and will be included in the liability total if there is still a liability balance indicated.

◯ **INCLUDED IN BANKRUPTCY** – The number of trade accounts included in a bankruptcy and the sum of the balance due segments for these accounts is reflected on this line.

◯ **FORECLOSURE(S)** – The number of foreclosures (including sheriff's sales and public sales) and the sum of the balance due segments for these accounts is reflected on this line.

㉒ **PREVIOUS HISTORY/PAST DUE TABLE** – This table reflects the number of accounts that were reported as having been previously 30 or more days past due in the trade account segment, counter and payment history columns for each trade account in the credit report. The first two digits of the counter reflect the number of times that account was 30 days past due; the second two digits reflect the number of times that account was 60 days past due; the third two digits reflect the number of times that account was 90 days past due; and the last two digits reflect the number of times that account was 120 or more past due. The payment history column located directly under the counter column lists the 12 month history of manner of payment.

Each digit represents a per month rating for the trade account:

1 = current
2 = 30 days past due
3 = 60 days past due
4 = 90 days past due
5 = 120 days past due, etc.

The most severe delinquency associated with each account contained in the previous history/past due table is only reflected one time. For example, if a given account was previously 30 days past due six times and 60 days past due two times, it would be entered as one account that was 60 days past due.

㉓ **ZIP CODE AREAS INCLUDED IN THE VENDOR SELECTION PROCEDURE** – These numbers represent the first 3 digits of the zip codes where the Subject either lived, worked or went to school that DSS entered for inclusion in the credit vendor selection procedure. The vendor selection software selects the credit vendor believed to have the best coverage in those areas. In the event no single vendor can provide adequate coverage for those areas, multiple credit reports are purchased.

THE FOLLOWING PAGES REPRESENT A TYPICAL DSS DETAILED REPORT OF CREDIT

① ② ③

CONTROL NUMBER: 999990041 99999DQ132241M2 NAME: CHEESE, CHUCK E. PAGE: 1

DEPARTMENT OF DEFENSE – DSS DETAILED REPORT OF CREDIT

④
NAME/ADDRESS

NAME OF SUBJECTS	SS#	DATE-OF-BIRTH	
CHEESE, CHUCK E.	123-45-6789	29 Feb 68	
ALSO KNOWN AS	SPOUSE	SPOUSE SS#	
	KIM		
CURRENT ADDRESS	CITY/STATE/ZIP		SINCE
BOX 6491 PO	PIZZA PL 44400		N/A
PREVIOUS ADDRESS	CITY/STATE/ZIP		SINCE
BOX 6491 PO	PIZZA PL 44400		N/A
PREVIOUS ADDRESS (2)	CITY/STATE/ZIP		SINCE
3510 WIMBERLY LN APT G	WINSTON-SALEM NC 88800		N/A

EMPLOYMENT

CURRENT EMPLOYER	CITY/STATE/ZIP	DT EMPL	SALARY
US ARMY	N/A	N/A	N/A
PREVIOUS EMPLOYER	CITY/STATE/ZIP	DT EMPL	SALARY
LEGGS	N/A	N/A	N/A
PREVIOUS EMPLOYER (2)	CITY/STATE/ZIP	DT EMPL	SALARY
USA	NC	N/A	N/A

DSS DETAILED REPORT OF CREDIT

CONTROL NUMBER: 999990041 99999DQ132241M2 NAME: CHEESE, CHUCK E.

SOURCE

(5) CREDITORS

CREDITOR NAME (6)			ID# (7)		KIND OF BUSINESS (8)	
ACCOUNT # (9)	PAYMENT MANNER (10)	PAST DUE (11)	BALANCE (12)	DATE OPND (13)	ACCT USER (14)	COUNTER (15)
			SHI CRDT (16)	LAST ACT (17)	ACCT TYPE (18)	PAYMNT HIST (19)
		TERMS (20)	STATUS/COMMENTS (21)			

C 1 1ST NAT BK (6) 6608800285 (7) BANKS (8)
9757905 (9) PAYS AS AGREED (10) -- $3905 7/95 (14) INDIVIDUAL 02010000
$8500 9/98 INSTALLMNT 111111321211
296/?

C 1 AMER EXP (11) 9060N00259 NAT'L CRED CARD COS.
37347 BAD DEBT $217 $217 (12) 4/88 (13) INDIVIDUAL 00000000
$217 (16) 11/92 (17) OPEN (18)
CHARGE OFF ACCT
(21) SUBJ. DISPUTES THIS ACCOUNT

C 1 AMER EXP 9060N00267 NAT'L CRED CARDS COS.
37347 PAYS AS AGREED -- $0 4/88 INDIVIDUAL 00000000
$0 12/91 REVOLVING

C 1 ASSOCIATES FIN 149FP00458 PERSONAL LOAN COS.
31000654606 30 DAYS PAST DUE $2713 7/89 INDIVIDUAL 00000000
$3462 5/90 INSTALLMENT
0037/$200

(22) (23)
C 1 ASSOCIATES FIN 416FP01729 PERSONAL LOAN COS.
36920804539 PAYS AS AGREED -- $0 7/89 INDIVIDUAL 11020000
$3462 10/92 INSTALLMENT 121112111321
(20) 0037/$200 (19)
CLOSED ACCOUNT

DSS DETAILED REPORT OF CREDIT

CONTROL NUMBER: 999990041 99999DQ132241M2 NAME: CHEESE, CHUCK E.

CREDITORS

SOURCE	CREDITOR NAME			ID#		KIND OF BUSINESS	
	ACCOUNT #	PAYMNT MANNER	PAST DUE	BALANCE	DATE OPND	ACCT.USER	COUNTER
				$HI CRDT	LAST ACT	ACCT.TYPE	PAYMNT HIST
			TERMS	STATUS/COMMENTS			

C 1 **USA FINCL** **906FP02273** **PERSONAL LOAN COS.**
178732147949 PAYS AS AGREED -- $0 8/89 INDIVIDUAL 12050200
$0 8/92 INSTALLMENT 2243343232122
371/?
CLOSED ACCOUNT
SECURED LOAN

C 1 **WHIRLPOOL FIN CO** **906FF00047** **SALES FINANCING**
20037848067 PAYS AS AGREED -- $0 3/89 INDIVIDUAL 01040503
$261 9/91 REVOLVING 1114314311315
10/?

(24)

CREDITOR CODES

TERMS - # MONTHLY PAYMENT/PAYMENT AMOUNT
COUNTER - 2 bytes each for 30 Days/60 Days/90 Days/120 Days Past Due
PAYMENT HISTORY - 12 Month History Of Manner of Payment
DATE LAST ACT. - Date of Last Account Activity

DSS DETAILED REPORT OF CREDIT

CONTROL NUMBER: 999990041 **99999DQ132241M2** **NAME:** CHEESE, CHUCK E.

COLLECTIONS (25)

CREDITORS (26)	STATUS (27)	ORIGINAL AMOUNT (28)	DATE FILED (29)	COLLECTION AGENCY (30)
ACCOUNT NUMBER (31)	DATE PAID (32)	$ BALANCE (33)	DATE RPTD (34)	ID # (35)
CL-89000 (26) 690025	UNPAID (27) (32)	$54 (28) $54 (33)	10/89 (29) 2/94	CSC CREDIT SERVICE IN 615YC01003
CL - 8900 764907 (31)	UNPAID	$124 $124	4/91 2/94 (34)	CSC CREDIT SERVICE IN 615YC01003 (35)

PUBLIC RECORD (36)

ACTION TYPE (37)	STATUS (38)	STATUS DATE (39)	$ LIABILITY (40)		DATE FIILED (41)
		COURT TYPE (42)	ASSETS (43)	DOCKET # (44)	JUDGEMENT DATE (45)
COURT = (46)		PLAINTIFF COURT ADDRESS (47)			
TAX LIEN (37)	(38)	(39) (42)	$294 (40) (43)		1 94 (41) (45)
655VC29142		CITY COUNTY BLDG INDPLS IN 46204			
TAX LIEN			$367		3 92
416VC00115 (46)		(47) 180 N IRBY ST FLORENCE SC 416 (48) SUBJ. DISPUTES THIS ACCOUNT		108-18	
TAX LIEN			$2,265	(44) 02027060	11 90
660VC07688		COURT HOUSE WARSAW IN 99999			

(49) **CONSUMER STATEMENT / MISCELLANEOUS INFORMATION**

(50) THE CHARGE OFFS ON MY REPORT ARE A RESULT OF MY IN. .BILITY TO SELL MY HOME IN INDIANA FOR 2 YEARS. COUPE WITH THE FACT THAT I HAD JUST GOTTEN DIVORCED, THIS CREATED HARDSHAIP, HOWEVER THE CHARGE OFF BY AMERICAN EXPRESS IS A RESULT OF A DISPUTE, I CLAIMED THAT I DID NOT OWE THEM THE MONEY & THEY WERE SUPPOSED TO INVESTIGATE MY CLAIM, THEY DID NOT CONVINCE ME THAT I OWED THEM THE MONEY, IT SEEMS AS THOUGH THEY GOT TIRED OF THE MATTER.

(51) MISCELLANEOUS INFORMATION

ACCOUNT NAME (52)	ACCOUT # (53)	PHONE (54)	ADDRESS (55)
1ST NAT BK AMERICAN EXPRESS	9757905 (53) 37347	N/A (54)	POB 1447 WARSAW IN 46580 (55) CALL 1-800-933-4056 FOR ADDRESS CUST# 801VF00572; SUB#: 9060N00259
AMERICAN EXPRESS	37347	MAIL ONLY	777 BRDWAY NY NY 10003
ASSOCIATES FIN	31000654606	N/A	201 S NAPANEE ST ELKHART IN 46515
ASSOCIATES FIN	36920804539	N/A	PO BOX 3099 FLORENCE SC 29502
AVCO FINANCIAL	13150948305950		CALL 1-800-933-4056 FOR ADDRESS CUST#: 801VF00572; SUB#: 906FP00509

DSS DETAILED REPORT OF CREDIT

CONTROL NUMBER: 999990041 999990Q132241M2 NAME: CHEESE, CHUCK E.

MISCELLANEOUS INFORMATION

ACCOUNT NAME	ACCOUNT #	PHONE	ADDRESS
AYRES	46339230		CALL 1-800-933-4056 FOR ADDRESS CUST#: 801VF00572; SUB#: 404DC00807
CENTERREBK	7111013041	N/A	CALL 1-800-933-4056 FOR ADDRESS CUST#: 801VF00572; SUB#: 154BB00256
CRDT FIRST	572089681	2163624000	6275 ELAND RD BROOK PARK OH 44142
CSC CREDIT SERVICES IN	690025	N/A	8500 SHAWNEE MISSI MERRIAM KS 66202
DINER	381765677201	N/A	183 INVERNESS DRIV ENGLEWOOD CO 80112
FASHONBUG	5856370580121805	6097724559	745 CENTER ST MILFORD OH 45150
GLHEC	493683376888888	N/A	2401 INTERNATIONAL MADISON WI 53704
LAKECITYBK	40060200872411		CALL 1-800-933-4056 FOR ADDRESS CUST#: 801VF00572; SUB#: 658BB10380
NBD CR LN	000807050012612		CALL 1-800-933-4056 FOR ADDRESS CUST#: 801VF00572; SUB#: 168BB24087
NBD SKOKIE	5180757050012612	N/A	8001 LINCOLN AV SKOKIE IL 60077
NCB/COLS	8840340725	N/A	4653 E MAIN STR COLUMBUS OH 43251
SLMA-LSCY	493683376104	8008829500	365 HERNDON PARKWA HERNDON VA 22070
SOURCEONE	3191515	N/A	CALL 1-800-933-4056 FOR ADDRESS CUST#: 801VF00572; SUB#: 168FM00010
TAX LIEN	108-18	N/A	180 N IRBY ST FLORENCE SC 416
TAX LIEN		N/A	CITY COUNTY BLDG INDPLS IN 46204
TAX LIEN	02027060	N/A	COURT HOUSE WARSAW IN 99999
USA FINCL	178728799928	N/A	1122 W BRISTOL STR ELKHART IN 46514
WHIRLPOOL FIN CO	20037848067	N/A	533 BENSON RD BENTON HARBOR MI 49022

END OF REPORT (56)

DSS DETAILED REPORT OF CREDIT

CONTROL NUMBER: 999990041 99999DQ132241M2 NAME: CHEESE, CHUCK E.

(57)

C1 EQUIFAX-CREDIT BUREAU OF WINSTON-SALE

711 COLISEUM PZ
WINSTON-SALEM NC 27106
PHONE: (910)777-3500

(58)

C1 Name: CHEESE, CHUCK E. SSN: 123-45-6789

(59) DOB : 29 Feb 68

Also Known As:

Current Address:	BOX 6491 PO PIZZA PL 44400	Since: N/A
Previous Address:	BOX 6491 PO PIZZA PL 44400	Since: N/A
Previous Address:	3510 WIMBERLY LN APT G WINSTON-SALEM NC 88800	Since: N/A
Current Employment:	US ARMY	Date Empl: N/A
Prior Employment:	LEGGS	Date Empl: N/A
Prior Employment:	USA NC	Date Empl: N/A
Prior Employment:	LEGGS	Date Empl: N/A
Prior Employment:	USA NC	Date Empl: N/A

① **NAC CASE NUMBER**

② **CASE CONTROL NUMBER**

③ **SUBJECT'S NAME**

④ **PAGE 1 OF THE CREDIT REPORT LISTS THE FOLLOWING INFORMATION OBTAINED FROM THE ACCESSED CREDIT SYSTEM**

– Subject's Name
– Social Security Number (SSN)
– Date of Birth
– AKA's
– Spouse's Name
– Spouse's SSN
– Current Address
– Previous Address
– Previous Address (2)
– Current Employment
– Previous Employment
– Previous Employment (2)

⑤ **TRADE ACCOUNT COLUMN HEADING** – The Column Heading will appear at the top of each page that contains trade accounts. Each trade account is listed alphabetically.

⑥ **CREDITOR NAME**

⑦ **CREDITOR IDENTIFICATION NUMBER**

⑧ **KIND OF BUSINESS**

⑨ **ACCOUNT NUMBER**

⑩ **MANNER OF PAYMENT**

⑪ **AMOUNT PAST DUE**

⑫ **ACCOUNT BALANCE**

⑬ **DATE ACCOUNT OPENED**

⑭ **ACCOUNT USER**

⑮ **COUNTERS** – 8 digits: 2 digits each for 30 / 60 / 90 / 120 days past due
(e.g. 01020001 = once 30 days past due; twice 60 days; zero times 90 days & once 120 days)

⑯

HIGH CREDIT

⑰ **DATE OF LAST ACTIVITY**

⑱ **ACCOUNT TYPE**

⑲ **PAYMENT HISTORY –** 12 month history of manner of payment, read from left to right. Each digit represents a rating per month for the trade account:

1 = current
2 = 30 days past due
3 = 60 days past due
4 = 90 days past due
5 = 120 days past due, etc.

⑳ **TERMS** – Number of monthly payments/payment amount

㉑ **ACCOUNT STATUS/COMMENTS**

㉒ **SOURCE SYSTEM ACCESSED FOR EACH TRADE ACCOUNT –**

C = CBI
T = TRANS UNION
W = TRW
(Also see ㊼)

㉓ **CREDIT INQUIRY NUMBER** – The number code will correspond to each item listed in the credit report (e.g. C1 – Identifies the system and bureau accessed for each item listed in the credit bureau report). (Also see ㊼)

㉔ **CREDITOR CODES INTERPRETATION SECTION**

㉕ **COLLECTION ACCOUNT COLUMN HEADING** – The column heading will appear when collection accounts are listed in the credit report.

㉖ **COLLECTION CREDITOR CODE**

㉗ **STATUS**

㉘ **ORIGINAL AMOUNT**

㉙ **DATE FILED**

㉚ **COLLECTION AGENCY NAME**

㉛ **COLLECTION ACCOUNT NUMBER**

㉜ **DATE PAID**

㉝ **ACCOUNT BALANCE**

㉞ **DATE REPORTED**

㉟ **COLLECTION IDENTIFICATION NUMBER**

㊱ **PUBLIC RECORD COLUMN BEADING** – The column heading will appear when public record items are listed in the credit report.

㊲ **ACTION TYPE** – Description of the Public Record

㊳ **STATUS**

㊴ **STATUS DATE**

㊵ **LIABILITY AMOUNT**

㊶ **DATE FILED**

㊷ **COURT TYPE**

㊸ **ASSETS**

㊹ **DOCKET NUMBER**

㊺ **JUDGMENT DATE**

㊻ **COURT IDENTIFICATION NUMBER**

㊼ **PLAINTIFF /COURT ADDRESS**

㊽ **NARRATIVE COMMENTS**

㊾ **CONSUMER STATEMENT /MISCELLANEOUS INFORMATION HEADING** – The heading will appear when a Consumer Statement or Miscellaneous Information is listed in the credit report.

㊿ **CONSUMER STATEMENT**

(51) **MISCELLANEOUS INFORMATION COLUMN HEADING** – The column heading will appear preceding the credit grantor identifications listed alphabetically.

⑫ **ACCOUNT NAME**

⑬ **ACCOUNT NUMBER**

◯ **PHONE NUMBER**

⑮ **ACCOUNT ADDRESS**

⑯ **END OF REPORT**

◯ **CREDIT SYSTEM AND BUREAU ACCESSED**

⑱ **PERSONAL IDENTIFICATION DATA**

◯ **SOURCE AND CREDIT INQUIRY NUMBER** – The code will correspond to each item listed in the report. (e.g. C1- identifies the system and bureau in the credit report accessed for each account listed to the system and bureau listed in item ⑰.)

HOW TO REVIEW CREDIT BUREAU REPORTS

Reviewing Reports of Credit Designed for the Defense Security Service

15 May 2001

Defense Security Service Academy
938 Elkridge Landing Road
Linthicum, MD 21090-2917
www.dss.mil/training

Security through Knowledge

15 May 2001